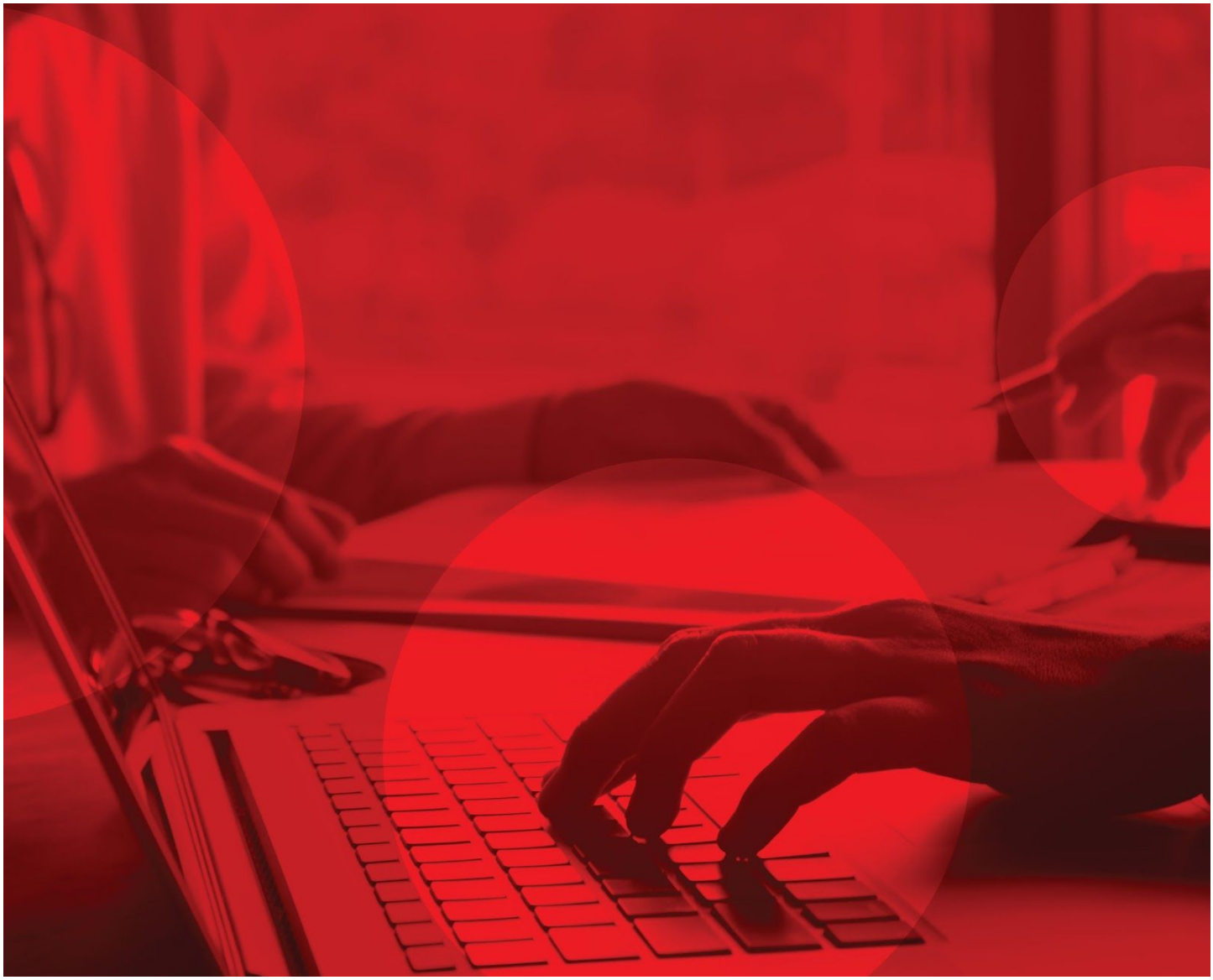
SCALED ACCESS

WHITEPAPER

Sharing Confidential Data Doesn't Require Sharing Credentials



Intro

Access Management tools play an important role in industries where confidential data such as medical, financial and insurance information is handled and shared. These tools ensure FinTech, MedTech and InsurTech employees can get access and share confidential data when collaborating.

Under current IAM implementations, employees are circumventing the system, sharing credentials and accounts to access confidential data. However, when employees share credentials it vastly increases security risks.

In 2019, Comodo, ironically a cybersecurity company, suffered a data breach due to a set of credentials being shared by multiple users getting exposed on the internet[1]

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

"Under current IAM implementations, employees are circumventing the system, sharing credentials and accounts to access confidential data."

They need to deploy a solution that lets employees securely and easily share access to confidential data without needing to share credentials.

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 having a designated set of access rights assigned to it.

[1] https://techcrunch.com/2019/07/27/comodo-password-access-data/

For example, a hospital may deploy an access policy where users who are doctors can view and update all sections of an electronic health record (EHR), whereas nurses can view all sections of an EHR, but only update limited sections. Or an insurance company may deploy an access policy where users who are insurance brokers can see all sections of an insurance claim, but insurance doctors can only see the medical section of the claim.

These traditional solutions require a lot of back-office administration. Depending on their deployment, back-office staff need to assign permissions, privileges, entitlements, access groups and authorisation roles to users.

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

- Onboarding new users
- Assigning new roles, permissions (etc.) when users' roles and 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 if they haven't done their job:

- New employees can't start working
- Employees who've been given a new role or tasks can't access additional data needed to perform their new responsibilities
- Ex-employees can still get 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 poses serious business and security risks to their company.

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 found that there are still companies who actually permit credential sharing, which 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 their credentials with co-workers[2].

Organisations must wake up and combat the legitimate problem that their employees are sharing credentials to access confidential data.

The Risks Of Sharing Credentials To Confidential Data

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

These risks include:

- The risk of credentials falling into the wrong hands, allowing outsiders to access this 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 unauthorised payment, delete sensitive data or could even change account

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

passwords, thereby locking other users out, all without anyone knowing which user did it.

- The risk of zero-accountability. If employees share credentials, it would be impossible to keep track of who did what. Who actually processed the insurance claim? Who authorised the payment? Who updated the medical information? If tasks are done incorrectly the company can face issues without being able to find out who was responsible.
- The risk of an ex-employee being able to access confidential data. While the credentials aren't changed, ex-employees can still gain access to company resources and sensitive company data. A study by Varonis[3], a cybersecurity company, on 785 organisations 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 costing vast sums of money 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 risks associated with doing so?

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

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

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.

Some practical scenarios that could result in employees sharing credential 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 analysis of 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 immediately re-evaluate their security policy.

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

Next-generation access 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 next-generation solutions are designed knowing that employees come and go, employees' tasks and responsibilities often change, and that employees require different access to data.

These solutions solve the challenges faced by traditional IAM implementation by delegating administration to the employees themselves, reducing back-office administration, saving time and money, and preventing back-office inefficiencies.

Companies can design access policies and these access platforms enforce them. This way employees can themselves invite others to get access to 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 needs updating.
- Employees no longer need access to specific company resources.
- Employees need to be offboarded.

To delegate administration to employees, these access 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 others when they no longer require access. Has the doctor moved departments? Remove the doctor from the team.

These platforms also provide peer-to-peer validation workflows that companies can customise to let authorised users approve someone else's invite or request for access. This lets 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 someone has invited another to gain access 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 authorised employees immediately withdraw access the ex-employee had, thereby protecting company resources by quickening the offboarding process typically done by back-office staff, which better secures the company resources.

Conclusion

In conclusion, next-generation access platforms provide solutions that remove the need and motivations for employees to share credentials and accounts to share access to confidential data. These solutions reduce reliance on back-office administration as they 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. Next-generation access solutions mean that effective collaboration no longer requires employees to share credentials, and that company policy no longer needs to endorse credential sharing to enable collaboration.

"Next-generation access platforms provide solutions that remove the need and motivations for employees to share credentials and accounts to share access to confidential data."