Controlling Access To Sensitive Data Without Causing Shadow IT

A Progress | Ipswitch eGuide

Progress® | ipswitch®

Introduction

When it comes to controlling where your sensitive business data in today's business landscape, there are many questions to consider:

- Is your data adequately encrypted with the latest protocols?
- Are your file transfer tools fast and efficient enough for your users?
- Are access controls in place that limits access to sensitive data?
- Can you back up all the above in the face of an audit?
- Have your users implemented strong passwords to access sensitive data?

If you can't answer any of the above with confidence, then you need to reconsider how you are protecting your data. Even if you don't work in healthcare, government, or finance, every business is in a regulated industry in some capacity.

The GDPR was just the beginning of data protection laws around the world. The USA is now implementing its own rules, even if it's only on the state level. Regardless of where your business resides and whatever industry you're operating in, you too are on the hook for protecting your employees' and customers' sensitive data.

It all starts with access control, but don't stop there. Your business will also need the highest standards in encryption with multi-factor authentication on top.

Controlling access to sensitive files, devices, tools, and network areas is of utmost importance in cybersecurity, but you should also know that it's not enough to simply control how users access resources. It's equally important to be able to track and audit access so that you can see who's logged on, when and where they did it, and the resources that they've accessed. That's where auditable access controls come in handy.

Then there is encryption. Encrypting that data at rest and in-transit is critical, but it does nothing if your users use weak passwords to access those systems.

You're a Regulated Industry and Need Access Control

Access control is especially important in highly regulated industries, such as healthcare or banking, where regulators will occasionally need to perform audits to prove that only authorized users accessed sensitive data, that they only did so when necessary, and that access and transfer of sensitive data was performed in a secure and compliant manner. But nowadays, more and more companies are on the hook regardless of the industry.

Principle Six of the GDPR, for example, states that data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

The GDPR was just the beginning of data protection laws around the world.

Those “appropriate technical or organizational measures” are essential, and you can bet that access controls are one of them, but if those access controls don’t leave an auditable log, you’ll have a hard time proving compliance to regulators.

Lacking that degree of visibility and logging required for compliance certification can result in significant consequences. The logs should be tamper-evident and keep track of when a file was transferred if the right party received it, and whether or not it was subsequently deleted.

...nowadays, more and more companies are on the hook regardless of the industry.

Maybe you argue that you don’t work in the confines of the EU. It may not matter to you at this very moment, but if you’ve been paying attention, other countries, including the US, are following suit. The cybersecurity epidemic sweeping companies across the world is a bipartisan issue which means progress is being made in regards to data protection legislation.

For example, in 2020 California will be enforcing its own California Consumer Protection Act (CCPA). This law is a lot vaguer than the GDPR, but it was still drafted with the GDPR as a considerable blueprint. And other states are following California’s example. There may not be a federal law in place, like HIPAA, but it’s only a matter of time. Why not get prepared and be proactive rather than the approach of wait and see what happens?

The Case for Powerful Access Controls

If you’re using secure file transfer tools, chances are you’re security conscious. Maybe you’re working in a highly-regulated industry, or perhaps you don’t want your company on the front page of the newspaper for getting hacked. Regardless of your industry, in addition to encrypting file transfers, you should lock down access to your secure file transfer tool as tightly as possible. But even though file transfer tools like FTP and email are generally encrypted, they aren’t perfect.

As stated earlier, controlling access to protected data is essential. However, there is a dark side to all this. Basic file transfer systems are an often-overlooked attack vector for cybercriminals. It goes without saying that access to these systems should be controlled. Passing an audit is fine, but it still doesn’t save you from actually being breached and fined in that regard.

As stated, access should only be granted to people that are required to use it as part of their job—not every employee or external partner needs access to all company information. This becomes harder when email and FTP is involved, for instance. Passwords are not always secure and many times already compromised by the time they are implemented.

It’s easy enough to control and enforce access by applying simple rules and policies, like strong password policies, but for a highly regulated environment like banking or healthcare, you want full control over user access and permissions as well as centralized user authentication.

But it possible to go too far with access control?

Too Many Restrictions Can Push Users to Shadow IT

One of the most persistent issues facing the modern IT team is the problem of shadow IT. Any IT pro knows that the unsanctioned use of cloud-based apps like Dropbox, Google Drive, and Evernote, is surging, and it can be a threat to the data security of any organization, not just your typical regulated industries.

Time and time again, employees with access to perfectly good secure file storage or file transfer tools turn to consumer-grade file-sharing tools like Dropbox and Google Drive. Why? Because employers often forget the importance of ease-of-use when it comes to internal apps.

We may be obsessive about our customer's user experience on our websites, but who cares if Mary in marketing has to take an extra few minutes to log in to transfer a file securely? Well, Mary cares. And if she can use Google Drive to move that file in the time it would take her to log in to your Secure File Transfer solution, you can bet she's going to do just that.

When we put too many restrictions on our users and make their user experience poor, they're going to turn to other options. Especially considering the fast-paced, collaborative atmosphere of many modern workplaces.

That's why shadow IT has become a persistent issue for organizations both large and small. Users are smarter than ever, and if you slow their workflow down, they're going to find ways to get that time back—and that could mean using tech outside of the tools offered to them. And the ubiquity of free file transfer tools only exacerbates the problem.

Unfortunately, these tools can be very insecure if set up improperly, and the free versions don't adhere to strict compliance standards that may be a necessity for your organization. But how do we get users to stop shadow IT?

In our computerized world, things tend to be reduced to binary as often as possible. 1 or 0. On or Off. Positive or Negative. Access Granted or Access Denied. That shouldn't always be the case.

It's easy for IT to get caught up in that mindset because that's how computers think and that's how you need to talk to them. But the real world isn't binary and it's important to get out of that mindset when determining permissions for accessing sensitive data.

If you're on-boarding someone who is going to be accessing files or folders that you've deemed secure, you almost definitely don't want to give them unlimited access to everything. Not only do new employees need access to everything, it's going to make it that much harder for you to keep that data secure, and to track down any leaks or breaches after they happen.

The goal for sharing any data should be to embrace granular permissions rather than access granted or denied. We also don't want to be so restrictive that an employee starts going rogue because it's taking too long to send and receive data.

...the real world isn't binary and it's important to get out of that mindset when determining permissions for accessing sensitive data.

Examples of Proper Access Control

Let's say John the tax preparation specialist has contracted with XYZ Corporation to prepare the taxes for all their employees. John can set up a shared folder with individual access for each employee and grant them only upload permissions.

The employees can't download or delete anything and they can't even list the files that are in the folder. This way John makes it easy for his clients to submit their protected financial information in one place while keeping all those files secure and private.

Mary is in charge of creating a marketing video for a major product launch a few months from now. She has a presentation that includes highly sensitive diagrams that can't be leaked before the launch, but she needs an external video production team to animate the presentation, a professional voice-over (VO) actor to read the script and a 3rd-party editor to put it all together. At the same time, there are multiple other internal employees that need to be able to review each iteration of the video and provide feedback during the process.

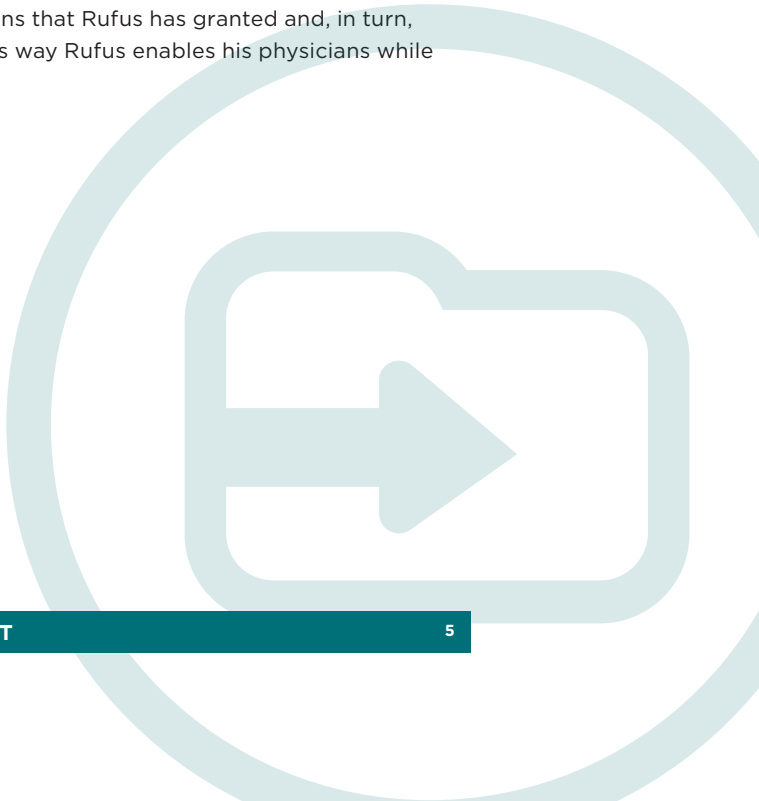
Mary can set up a folder that lets the video production house download the presentation and upload animations. The VO artist can only upload audio tracks and can't see any other files, ensuring he's not exposed to the sensitive diagrams. The editor can see and download everything while uploading the finished product.

None of them can list the other users of this folder. Mary and her coworkers can, however, and they are able to provide feedback to each individual vendor without exposing privileged information.

Rufus manages IT for a large healthcare organization and is responsible for ensuring that protected health information (PHI) stays secure. However, there's a team of physicians that often need to send patient information to external specialists on an ad hoc basis. Rufus can enable this team to create their own shared folders for third parties with limited permissions.

The radiologist may only want to securely send images to other specialists, granting them download rights only. The hematologist may need to collaborate with multiple specialists on blood test results which will require them to download and upload PHI. Another physician is just sending billing information to different insurers every day and needs to be notified when they download them.

Each physician can create a shared folder only with the permissions that Rufus has granted and, in turn, those who access that folder gets only the same permissions. This way Rufus enables his physicians while avoiding HIPAA violations.



Proper Tools Equal Proper Outcomes

The solution to all of the above examples isn't complicated: simply ditch outdated and insecure file transfer methods. Standing up FTP servers may have worked in the past, but it's simply insufficient in the age of the CCPA, GDPR, and HIPAA.

With a proper managed file transfer solution, you can quickly get complete visibility and control over file transfer activities between partners, customers, users, and systems. Secure files at rest and in transit and assure compliance with internal policies and regulatory mandates.

MOVEit, for example, boasts advanced security features including FIPS 140-2 validated AES-256 cryptography, users authorization / authentication, delivery confirmation, non-repudiation, and hardened platform configurations. MOVEit Transfer logs activities in a tamper-evident database to comply with ISO 27001, HIPAA, PCI, GDPR, SOX, BASEL I/II/III, FIPS, FISMA, GLBA, FFEIC, ITAR and data privacy laws. It also integrates with your existing DLP and anti-virus systems, identity systems through SAML 2.0, AD, LDAP services, and SIEMs. Additionally, MOVEit offers API interfaces (including REST) for integration with other third-party applications.

Trust us, all the extra encryption and audit trail that a managed file transfer solution provides is great, but there is one caveat. If a user's password is stolen, then all of this security goes out the window. That's why the multi-factor authentication (MFA) built into your managed file transfer solution is also critical.

The Problem with Passwords and Encryption

Even using a password manager that generates random, lengthy passwords isn't going to make a significant difference – and that raises other concerns like usability and creating a single high-value target. It's incredibly likely that your users' passwords are already in the list of the 500 million common passwords that hackers are continually testing against, so they're going to be just one of those 300 million accounts they hit each day. And that's assuming they aren't explicitly targeting your users. If so, it's going to be even easier for them to hack them via phishing, keystroke logging, local discovery or some other method. The numbers don't lie, and you and your end users' passwords don't matter.

All that encryption may make your auditor happy and your business compliant to the patchwork of new laws, but it still does nothing if you just use passwords to protect those systems moving that data.

The Solution Isn't Compromise—It's Better Tools

The real solution is simple, and it doesn't involve compromising your security: If you want your employees to work in a secure manner, give them the tools that they need to do so, and make them easy to use. When you find a solution that accomplishes what they need to do, and that makes it as easy as possible to boot, then you've removed any bottlenecks from the process, and you won't have people straying to other tools.

Most people know that, where sensitive data is concerned, consumer-grade file-sharing solutions won't do. You need a Managed File Transfer tool like MOVEit, which can secure your data, with end-to-end encryption in transit and at rest, as well as access controls and audit trails that allow you to manage who is allowed to access and transfer sensitive data.

In addition, MOVEit provides multi-factor authentication out of the box, so that you don't just have to count on your end users implementing secure passwords. That's why MOVEit is the full package in providing a reliable and collaborative solution, with all the security and logging mechanisms that will get you through an audit.

For Your Free Trial of MOVEit Visit:
https://www.ipswitch.com/forms/free-trials/moveit

About Progress

Progress (NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, the flexibility of a cloud-native app dev platform to deliver modern apps, leading data connectivity technology, web content management, business rules, secure file transfer, network monitoring, plus award-winning machine learning that enables cognitive capabilities to be a part of any application. Over 1,700 independent software vendors, 100,000 enterprise customers, and two million developers rely on Progress to power their applications.

Learn about Progress at www.progress.com or +1-800-477-6473.