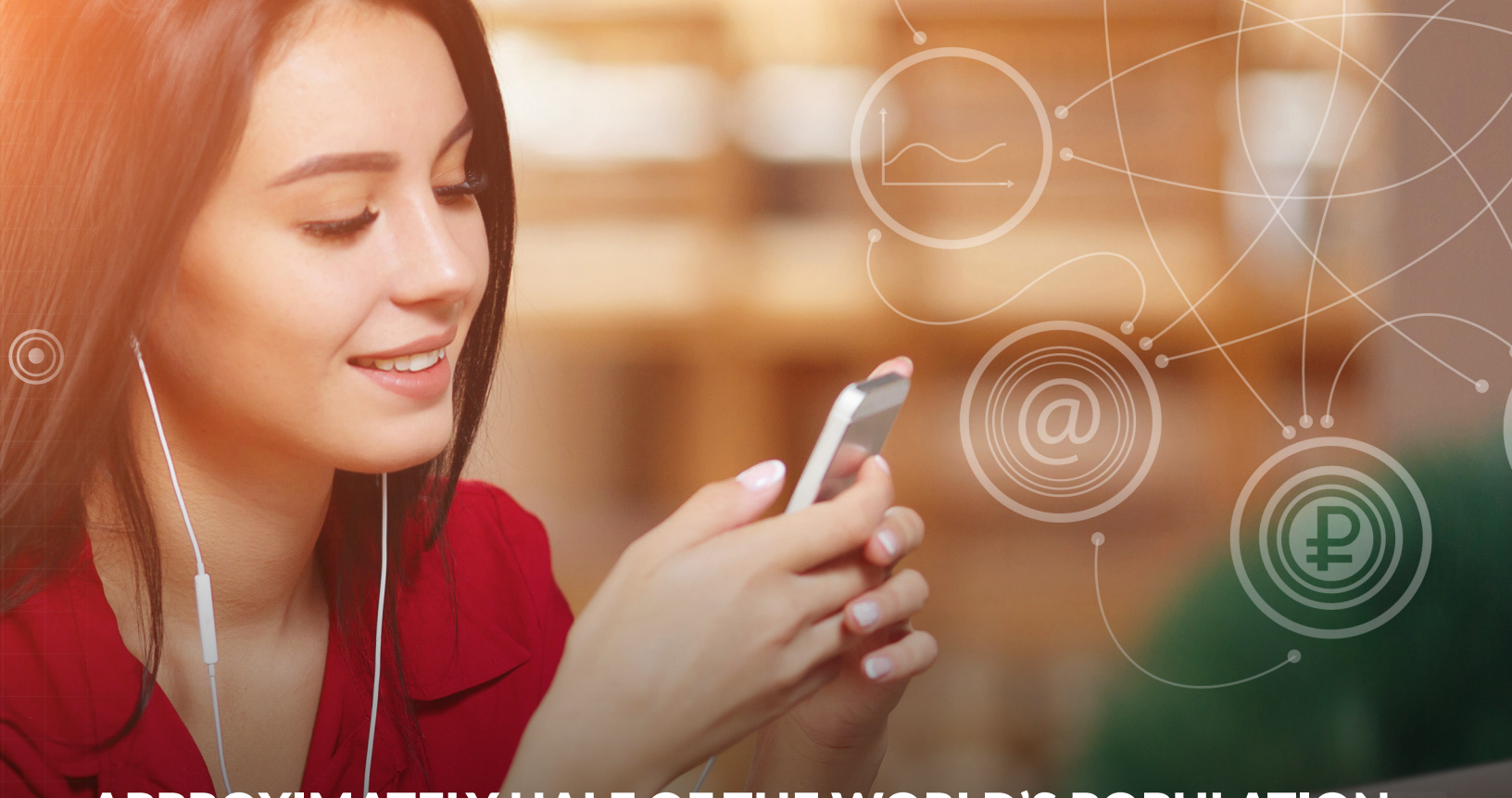
Red River

HOW MICROSOFT'S

AZURE INFORMATION PROTECTION CAN PROTECT YOUR ORGANIZATION



APPROXIMATELY HALF OF THE WORLD'S POPULATION IS ONLINE; THAT NUMBER IS MUCH HIGHER IN DEVELOPED COUNTRIES.

Consumers trust websites and online companies with gigabyte after gigabyte of personal data — credit card and social security numbers, addresses, images and videos, search history, and that's just a start. It's no wonder that a Statista survey found that, of all potential online issues, internet users in the United States were most concerned about having their data stolen.

As people share increasing levels of private, personal data with organizations and businesses, they expect that said data will be protected. Companies that expose consumer data can face significant liability, especially following the implementation of the European Union's General Data Protection Regulation (GDPR). Under the GDPR, exposing private data could cost a business €20 million or 4% of its annual income, whichever is greater.

The penalty is designed to be punishing; most businesses cannot easily absorb that cost. This comes on top of the cost of the data breach itself. A 2018 IBM/Ponemon study found that the average worldwide cost of a data breach was $3.86 million, rising to $7.91 million when only including organizations in the United States. Every individual person's data exposed costs a U.S.-based organization, on average, $233.

ACCORDING TO THE STUDY, THIS COST INCLUDES:

- Activities to detect and report a breach, like forensic and investigative activities, assessment and audit services, and crisis team management;
- Activities to notify individuals who have had their data exposed, like phone calls, emails, or letters;
- Legal expenditures, product discounts, issuing new accounts, credit-report monitoring, and helping customers through the process;
- Cost of business disruption and revenue losses from downtime.

Perhaps the biggest cost of a data breach, however, can't be easily measured in terms of financial impact: the damage a breach does to your organization's reputation and image. Learning that a company you trusted has exposed you to identity theft is a terrible spot for any consumer to be in, and many of those customers will leave your business for a long time if they ever return at all. The human cost of data breaches can be immeasurable.

While the public conception of a data breach typically involves hackers stealing information out from under an organization's proverbial nose — and indeed, malicious external threats certainly exist — an equally major cause of data breaches is much less sinister: Accidental, unintended data breaches caused by employee error. A Beazley study of data breaches found that while hacking or ransomware attacks caused 32% of all data breaches in 2017, accidental breaches were right behind at 30%.

Of course, to a customer, whether the breach was accidental or malicious doesn't matter, nor should it matter to you. Protecting sensitive information must be key for any organization — fortunately, there are excellent tools that help safeguard against both types of data breaches. One of the best of these tools is Microsoft's Azure Information Protection.

WHAT IS MICROSOFT AZURE INFORMATION PROTECTION?

Azure Information Protection (AIP for short) is a cloud solution offered by Microsoft as part of its Azure suite, which helps organizations protect potentially sensitive information in documents and emails. AIP is designed to work the way most modern businesses do, supporting mobile access, cloud-based authentication, and varying templates — also known as scoped templates — from department to department.

AIP is separate from the Active Directory Rights Management Services (AD RMS) that Microsoft has previously offered. Notably, AIP doesn't require any additional servers or public key infrastructure (PKI) certificates and is a wholly cloud-based solution. Given that AIP is a Microsoft-offered solution, it is primarily designed for integration with the Office 365 ecosystem of apps, but also supports a number of web solutions on the user's end.

Through the AIP Scanner tool, an organization can identify sensitive data in its network wherever that data lives, even in well-buried files and folder trees that have long ceased to be actively used. The scanner's ability to detect sensitive information, such as credit card or Social Security numbers, ensures that an employee will never be caught off guard and send an old file that they didn't realize contained protected data. But how does AIP enforce this protection?

BEHAVIORAL SECURITY VS. AUTHORIZATION-BASED SECURITY

There are two main ways that Microsoft AIP aims to protect data that you wouldn't want to leave your organization. The first is a behavioral framework. IT professionals have known that human error is one of the largest threats to proper information security for ages, and AIP aims to minimize the chances that a member of your team will be the source of an accidental data breach.

The AIP framework provides a way to add labels and levels of classification to all supported documents and emails; this can be automatic, as with the AIP Scanner tool, or manual. A user can flag a file, whether PDF, Word, Powerpoint, or any number of other supported file types, according to how sensitive the information it contains might be. This doesn't have to necessarily be protected data, like a credit card number, but can rather be data that your company might not want to get out, such as quarterly plans or internal financial numbers.

Once a document has been categorized, from Public-level information that is safe to send to anyone to Highly Classified-level information that should only be seen by a few, a user within the AIP framework will be able to easily check this status and will be notified if, for example, trying to email the file to someone else.

The scanner can also detect potentially sensitive information in a new file and suggest appropriate classification. This eliminates much of the need for guesswork on an employee's behalf and ensures accountability while reducing the risk that a document will be sent outside of the organization to someone who shouldn't be seeing it.

However, as anyone who works in information security will know, there is no such thing as an absolutely foolproof precaution. While the classification and labeling framework is designed to dramatically reduce the likelihood that an employee might accidentally send sensitive information outside of your organization, it cannot 100% eliminate it altogether. Labels may be applied incorrectly, an overburdened employee may overlook the warning, or the file may not be intentionally sent at all — for instance, perhaps it was left on a USB drive which fell out of an employee's bag.

This is where AIP's second method of information protection comes into play: an encrypted, authorization-based framework. Accidental data breaches are often compounded by a lack of encryption on the files in question, and AIP's architects are very familiar with this.

In addition to its behavioral framework designed to inform employees about the data contained in files or emails, Azure Information Protection supports an authorization-based framework using Microsoft's Azure Rights Management (Azure RMS). This aspect of AIP is fully integrated with the Office 365 suite and Azure Active Directory, and uses encryption, identity, and authorization policies; when you classify a document as having potentially sensitive data, AIP is able to detect who is trying to open the file and whether or not they have the authority needed to do so; with its powerful 2048-bit encryption key, AIP and Azure RMS, it virtually assures that only a person with said authority can access the data in question.

The encryption/authorization aspect of AIP is designed to be fully configurable on a document-by-document basis. For instance, you may decide that a sales forecast should be viewable by any member of your organization, but read-only aside from a select few users empowered to edit the file. However, should the file be left on a wayward USB drive or accidentally attached to an email through user error, someone outside your organization without the proper authority would not be able to open the sales forecast at all.

In a modern business environment, of course, you may have a need to share otherwise-sensitive information with people outside of your organization, such as business partners or trusted vendors. In that case, it's understandable that an overly restrictive system might not be too appealing.

Fortunately, AIP supports this use case: With its email integration, you can send protected emails to a user outside of your organization — or even to an employee's personal email, such as a Gmail or Hotmail account — and still be assured that your organization's sensitive information will be kept safe. A recipient whose email client does not have the authority to open a protected email can be sent a one-use passcode to see the message in a browser. Furthermore, you can select a classification setting that prevents emails from being forwarded, so your trusted vendor doesn't accidentally send information that they didn't realize was proprietary to someone you didn't intend to see it.

Between this authorization-based framework and the behavioral framework that notifies employees at a glance who should see documents or information, your organization's data will be much more protected than before.

AIP AND OFFICE 365

When considering information protection plans for your organization, one major strength to adopting AIP as a solution is how closely it's integrated with the apps in the Office 365 suite, which many organizations are already intimately familiar with. This makes adopting Azure Information Protection a fairly smooth integration for any organization already in the Office framework.

When using AIP with the Office 365 suite, the protection/classification bars will be natively added to the core Office apps, like Excel, Powerpoint, Word, and Outlook. Once you have properly configured your labels and run the AIP Scanner tool, identifying sensitive information and protected documents, your employees and team members will be able to start using AIP's protection right away.

In fact, some of Azure Information Protection's most useful features, like sending encrypted emails to someone outside your organization, require Office 365 Message Encryption (OME). However, AIP also supports S/MIME encryption, so even if you aren't using the Office 365 suite, your data and emails can still be protected.

WHAT ARE THE LIMITATIONS OF AIP?

For all the power, security, and use that Azure Information Protection provides, it — like all solutions — is not without its drawbacks.

Most prominently, AIP struggles to accommodate a situation wherein an organization is attempting to share protected data with external partners who aren't using the most recent versions of Office 365. Many organizations have not yet updated their toolset and are still using Office 2010; if your external partner has not switched to Office 2013 or newer, they will have to follow a series of steps to access a protected email you are trying to send them. While this is not a particularly strenuous series of steps, it is still an obstacle in the path of AIP working completely smoothly.

Similarly, there is currently no easy way for a regular employee to assign an AIP label to a new external partner. Since normal users cannot create contacts in their Azure Active Directory, they must ask someone with administrative powers to add a new contact before a label can be applied and documents can be shared with a new partner, vendor, or contractor.

AIP also currently lacks a native Azure Information Protection app for MacOS, so any business in a Mac environment will have to use the older RMS sharing app.

AIP: A POWERFUL, EFFECTIVE SOLUTION FOR NETWORK SECURITY

Despite some pain points and room for improvement, which are unavoidable for a solution as ambitious and comprehensive as Microsoft is hoping to build, there is no doubt that Azure Information Protection is a critical, useful tool to have in any organization's toolbox.

Its home in the cloud and lack of requirement of a dedicated server framework make AIP incredibly scalable, having great value for an organization of any size, from startups with a handful of employees to the largest enterprises.

Through its twin tracks of emphasizing behavioral security, which helps mitigate user error, and authorization-based security that ensures the only people opening files have the authority to do so, your organization can rely on Microsoft Azure Information Protection to protect your data. This mitigates legal liability and improves customer trust in your organization.

To learn how you and your organization can get started using AIP today, Contact Red River.com to learn more. Our experts will guide you through the process of putting this powerful solution to work for you.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.