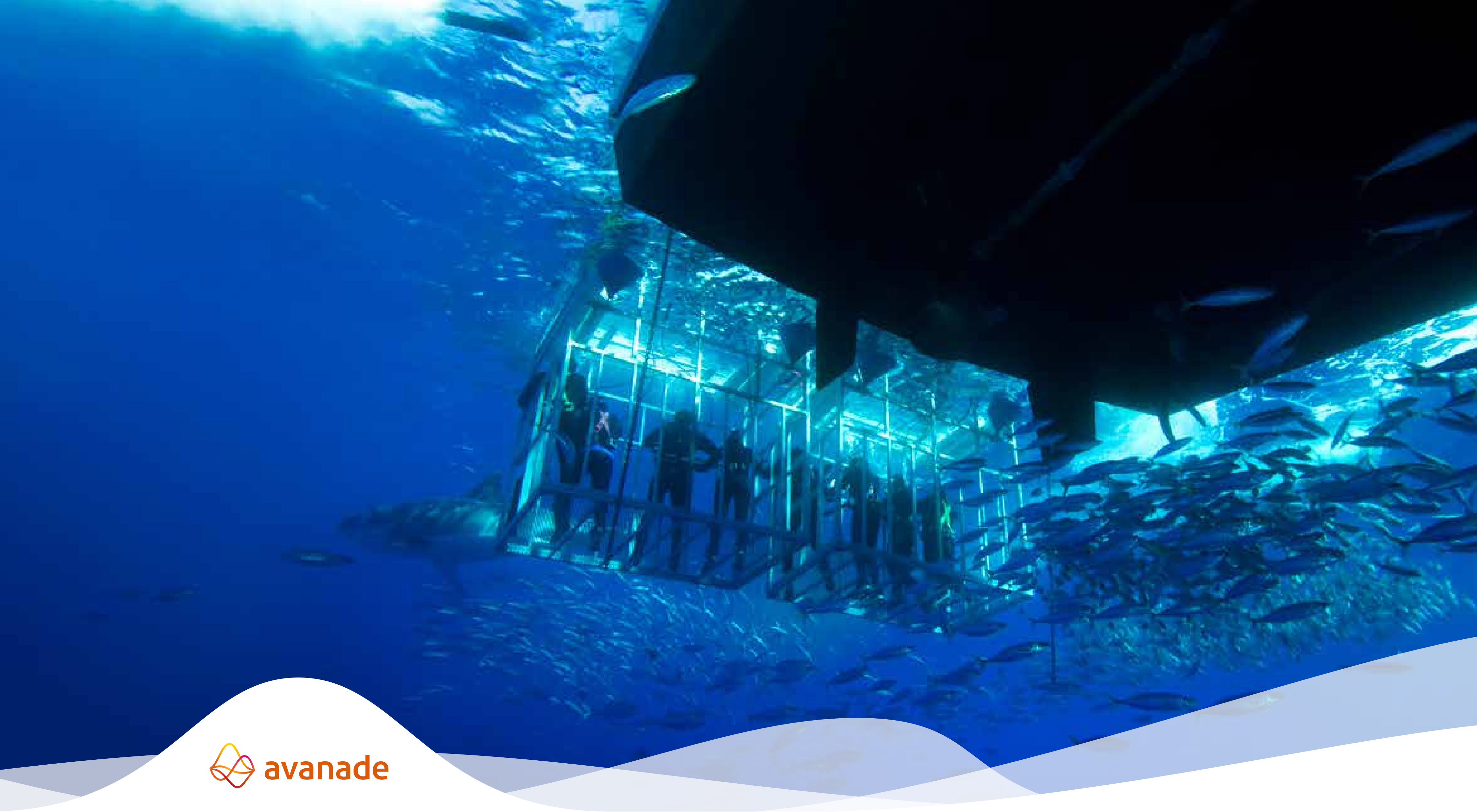


avanade

Secure your collaborative partnerships.

Drive greater efficiency and protection with secure 3rd party communication.

Your world is big.
That's how we think.

Let business flow – securely

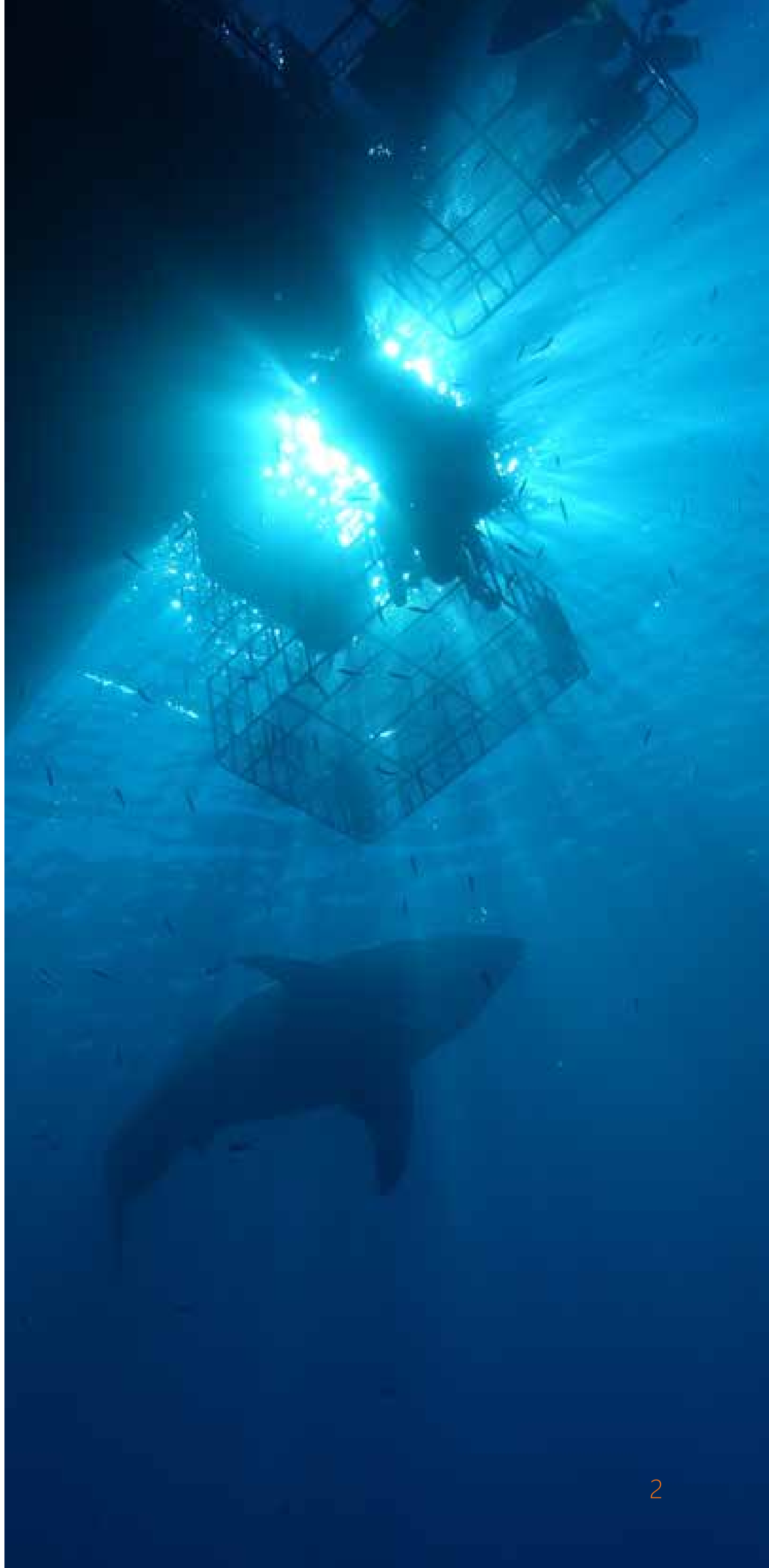
Enabling efficient collaboration between businesses is crucial to success in today's competitive and changing business environment. But how do you make sure every engagement is secure, each user is trusted and all files are shared safely?

The answer is a secure third party collaboration solution

Once you've hit send on your valuable information, or granted access to your IP, you have no control over what happens next.

Even if you trust a third party, your data is at risk as soon as it is shared outside of your organisation. Without sufficient controls in place, your data could be shared with others without your consent or knowledge. In a worst-case circumstance, if that third party is breached, your data could also be stolen and exposed along with the third party's own data.

In this guide, we explore the reasons why a secure third party collaboration solution is now key to your business' success.



Manage identity and access for confident collaboration

Secure third party collaboration solutions facilitate safe content and file sharing, reliable information protection and secure email encryption. But that's not all...

Optimise the way you collaborate

Third party Identity and Access Management (IAM) offers your business and employees the tools and technologies required to control user access to business information. It helps you define and manage the roles of individual users and their privileges, while providing automation to reduce the costs of managing third party identities. Consequently, you can optimise the way your staff collaborate by enabling them to share with trusted and verified identities – while reducing overall costs and becoming more agile.

GDPR and beyond

Secure third party collaboration solutions help you meet increasingly rigorous compliance requirements – such as the requirement to protect personal and sensitive information under the new GDPR regulation. But it doesn't stop there. IAM, for example, goes beyond GDPR to future-proof your corporate collaboration strategies and processes as your business continues to move forwards.

The benefits of secure third party collaboration solutions at a glance:

- Prevent the loss of sensitive business information or IP (Intellectual Property)
- Reduce overheads – especially when implementing a delegated IAM approach and enabling your trusted third parties to bring their own identities
- Improve identity-driven security by achieving a source of authority for third party identities
- Support GDPR readiness by protecting personal and sensitive information from loss and theft, mitigating the impacts caused by a breach with assurance that the information is protected

The challenges of managing identity and access

The biggest challenge to safe collaboration is when third party identities are required.

Obtaining access can take days if a well-established process isn't in place. Plus, access can often be granted but forgotten. That's not all...

What happens next?

Traditionally, once a third party receives a sharing link, anything could happen with the data being shared. When access is given via an email address, there's no assurance the recipient are who they say they are, and no insight into how they are using and consuming the information being shared.

When the third party gets the information they want, you have little out-of-the-box control over what they can do with it. How will they use it? Will they use it for means beyond what was intended? Even if you trust the third party, what if they have no means of managing themselves adequately? There's a lot to consider. What's more, how will you convey a sense of increased security as a positive thing, not a negative?

Overcoming the challenges

Many businesses find third party secure collaboration challenging to manage as it requires complex, people-driven processes that take up time and resources during every engagement. Across the space of a year, it all adds up. We've encountered these challenges with many of our clients. So, we've developed an approach to help...

Securely share what you need to, when you need to

We can help you securely collaborate with third parties – giving you the security and flexibility to optimise the way your business collaborates. We can transform how you approach third party identity management and how you manage third party access to your key assets.

Avanade secure third party collaboration

Our third party identity management solution allows you to delegate the administration of third party users to administrators within each of your trusted third parties. It enables group-based access control, which can be used to assign third party access at scale. It provides assurance that the identities that appear in the well known people pickers in tools such as Office 365 are well managed – and have been through a business and security approved identity proving process to validate they are who they say they are. It facilitates users' interactions with your business, including employees, contractors, partners and customers, with ease.

With a trusted identity in place, we leverage the capabilities of Azure Information Protection, Office 365 Message Encryption and Office 365 Data Loss Prevention. This enables the collaboration with your trusted third parties to be carried out in a secure way, providing best-in-class information protection when:

- Collaborating through SharePoint and Team sites – ensure information is protected when downloaded and taken offline so only site members have access, and apply further restrictions around printing and copying information when it is taken offline
- Authoring new information in Microsoft Office – apply protection through labels that not only clearly mark the document, but also quickly enable your departments to share securely with trusted third parties
- Sending personal or sensitive information – wrap the content in an Office 365 message encryption 'bubble' to ensure the information never leaves the safety of your controlled environment
- Accidentally or intentionally attempting to send internal confidential information externally – we can leverage Data Loss Prevention to prevent the information from ever leaving your environment

There are four key pillars to our offering:

1. Delegated business to business IAM
2. Collaborate securely with SharePoint, Teams and Office Pro Plus with Azure Information Protection
3. Secure email on any device with Office 365 message encryption
4. Prevent internal confidential information from being shared using Office 365 data loss prevention

Pillar 1

Delegated business to business IAM

For the partners you already trust, it makes sense to delegate business to business IAM to them. It'll help you maintain security while reducing admin costs.

- Know and trust third parties
- Delegate B2B IAM to trusted partners
- Enable partners to bring their own identity with Azure AD B2B
- Apply and manage end dates for identities
- Automated Joiners, Movers and Leavers
- Manage third party access at scale with group management

- Recertify access
- B2B Identities created in corporate Azure AD via high assurance confirmation process
- Reduce admin costs for 3rd party identities
- Lowers barrier to adoption – more accessible
- Increases user experience – ease of use

avanade

Pillar 2

Collaborate securely with SharePoint, Teams and Office Pro Plus

Let business information flow with SharePoint and Teams by assigning partner user access directly from the people picker. With our approach to third party IAM you can clearly identify third party users in your directory and have the assurance that they are well managed, and have been created via a confirmation process that's convenient and reassuring.

Create new information, specifically with the intention of collaboration in mind, by using Azure Information Protection labels. This means your departments can select a label to match each of your business processes – such as external collaboration with a third party legal counsel, or marketing company. Once the correct label is selected, the third party can receive and collaborate on your documents securely, with the risk of data loss or data leakage greatly reduced.

High assurance B2B Identities available in people picker

Folder sharing with selected assured partner identities

Files downloaded are protected with Information Protection

Author new information and clearly mark it for it's intended purpose

Quickly and easily protect information with "single click" protection via Azure Information Protection labels

Classify data according to labels, automatically or by user choice

Labels include access control lists enabling access to trusted external parties and Azure AD groups containing internal and external (B2B) users

Information emailed to approved 3rd parties is access and tracked

If information is shared to non-approved recipients access is denied and logged

Can be at an individual or organizational level

IT admin sets labels, policies, templates, and rules

Pillar 3

Secure email on any device with Office 365 message encryption

Send and receive encrypted email messages between people inside and outside your organisation to ensure that only intended recipients can view your sensitive content.

- Protected information emailed to partners
- Message protected with Office 365 Message Encryption (OME)
- Recipients receive OME link to secured email service
- Message content is consumed in secure web session
- Information never leaves your environment

Pillar 4

Prevent internal confidential information from being shared using Office 365 data loss prevention

Prevent internal confidential information from leaving your environment through data classification using Azure Information Protection Labels and the preventative controls available in Office 365 data loss prevention.

- Mark and protect all corporate information quickly and simply using labels
- Prevent the loss of internal confidential information through data loss prevention
- Define data loss prevention policies around your information classification taxonomy
- Only share what you want to share whilst providing protection from accidental or intentional data leakage

avanade

Summary of the key benefits of our approach

- Protection can be applied directly to documents with governance baked in – so only permitted third parties are able to interact with the protected documents
- Protection can be applied at the SharePoint library, OneDrive and Teams level enabling information to be protected at the point of download – ensuring any large libraries can still provide protection for documents, while enabling collaboration and modern ways of document editing
- Communicate securely with trusted third parties, ensuring content is protected and accessed securely regardless of the device or operating system the third party is using
- Assign application access and licenses to B2B identities while enabling application owners to review who has access to their applications on a periodic basis, supporting both security and compliance controls
- Provide a source of authority and management for business to business identities and manage their access to multiple applications across your Azure Active Directory
- Apply joiners, movers and leavers processes to B2B identities, ensuring they are fully managed throughout their lifecycle
- Only share what you want to share whilst providing protection from accidental or intentional data leakage

Benefit from our security expertise

Avanade has unparalleled expertise with Microsoft products, technologies and solutions, and we leverage that experience to advise you on the geographic data privacy obligations and security control requirements where you do business.

Our expertise includes:

- 65,000 Microsoft-trained professionals in Accenture and Avanade
- 24,000+ certifications in Microsoft technology
- 10,000 projects successfully delivered for over 4,000 clients worldwide
- 90+ Microsoft partner awards
- 17 Gold Competencies
- 13-time winner of Microsoft Partner of the Year

Let us help your business flow – securely

We can provide the secure third party collaboration systems that are right for your business, and help you manage the transition with ease.

Contact us to find out more.

www.avanade.com/security

Avanade is the leading provider of innovative digital and cloud-enabling services, business solutions and design-led experiences, delivered through the power of people and the Microsoft ecosystem. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation and has 30,000 professionals in 24 countries. Visit us at www.avanade.com.

[1] Wakefield Research: Avanade Hot Topics Survey, QuickRead Report, December 2017

avanade

avanade