A new approach to security

Over the past decade, cloud computing has soared in popularity.

50% **of all corporate data** is stored in the cloud

85% **85% of businesses** store sensitive data in the cloud

Working in the cloud requires a new approach to security – and Microsoft has been widely accredited for its role in leading this new approach.

In fact, the company has been named a leader by Gartner in four separate technology areas:

- Access Management
- Unified Endpoint Management
- Cloud Access Security Brokers
- Enterprise Information Archiving

For businesses looking to stay secure in a cloud-based, remote working world, Microsoft security offers some of the best possible protection.

Microsoft Security: Where to start

For those looking to get started with Microsoft security technology, there are three main areas to be aware of.

Identity and Access Management

Make sure the right users are logging into a customer's IT environment, no matter what device or location they're working from.

Technology includes: *Azure Active Directory, Conditional Access, Multi-Factor Authentication, Single Sign-On*

Threat Protection

Proactively identify and respond to new threats, taking advantage of Microsoft's global visibility over real-time attacks as they emerge.

Technology includes: *Advanced Threat Analytics, Microsoft Defender*

Information Protection

Create labels for sensitivity that live in documents themselves, ensuring information can't be shared or seen by the wrong people.

Technology includes: *Azure Microsoft 365 Information Protection, Microsoft Cloud App Security, Windows Information Protection*

Contact us

Through Microsoft Security technology, businesses have access to a formidable suite of effective security protections built for the cloud-first world.

Ready to get started? Get in touch with our experts today.