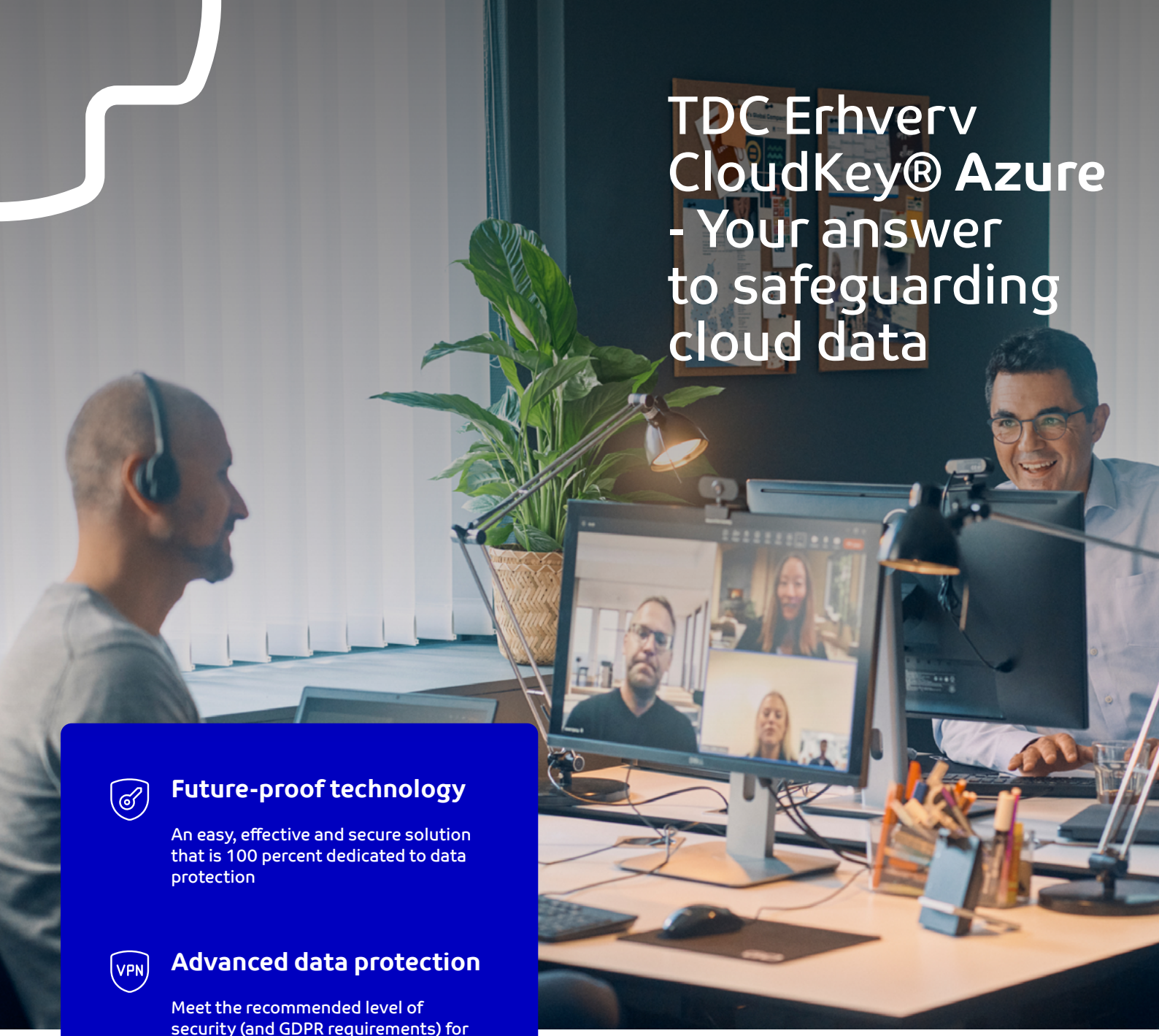


TDC Erhverv CloudKey® **Azure** - Your answer to safeguarding cloud data

Future-proof technology

An easy, effective and secure solution that is 100 percent dedicated to data protection

Advanced data protection

Meet the recommended level of security (and GDPR requirements) for your cloud services.

No superfluous investments

Full compatibility, allowing you to continue using your Microsoft licenses – without the day-to-day data security concerns.

A competent partner

Security and critical infrastructure are the cornerstones of TDC Erhverv. We will apply these skills to design, maintain and update your solution.

Microsoft Azure is a popular cloud service for companies and organizations everywhere. However, Microsoft is an American company, and thereby a so-called third country. This means that Microsoft can be obligated to provide the American authorities with access to their dataset. However, TDC Erhverv CloudKey® for Azure provides your data with an additional layer of security, so that you, and your business are protected. TDC Erhverv CloudKey® for Azure ensures that your cloud service providers cannot read your data.

TDC Erhverv
Se fremad

How does TDC Erhverv CloudKey® for Azure work?

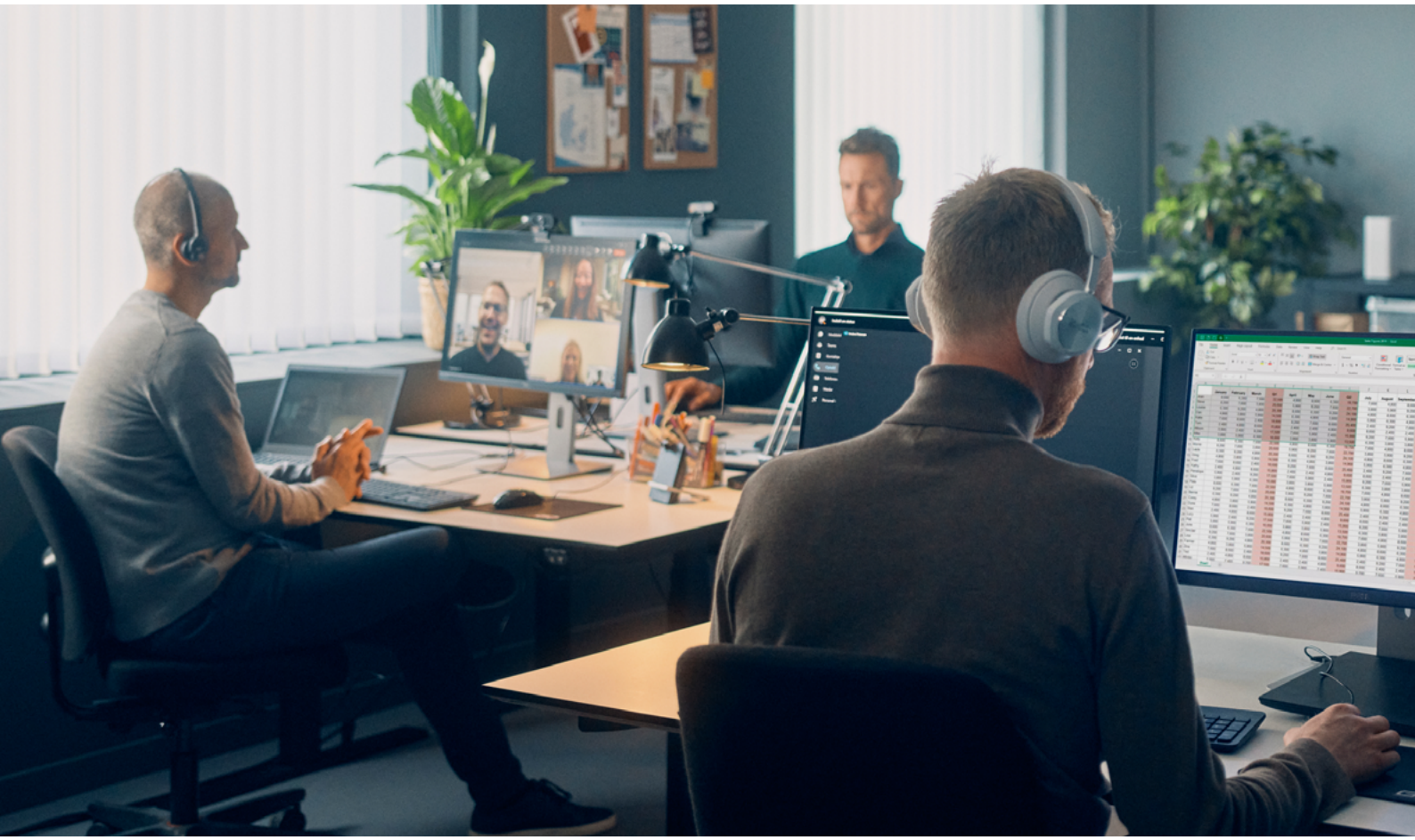
TDC Erhverv CloudKey® for Azure is designed together with Intel, who have developed a method to encrypt in motion data on a CPU memory level. Intel SGX oversees control access to the customer- and container´s application. At the hardware level, an enclave is implemented which secures the data on a CPU memory level.

The specific container-image is 'encased' using the TDC Erhverv CloudKey® for Azure toolkit. The agent will contact the Remote Attestation service of the TDC Erhverv CloudKey® for Azure when the container is started. This service will initiate a series of checks, e.g., the hardware behind the container platform is verified. When approved, the container will continue its start sequence and the application will open. The data integrity check is monitored by TDC Erhverv Security Operations Center (SOC).

The 'Enclave' – a secure and isolated domain – ensures that data is not available in plain text, while it is processed in-motion. In addition, the Enclave generates a unique key linking the application with the Enclave, so that only the application can access data in the Enclave. Access to the Enclave is integrated into the application.

The process is verified in the application by the TDC Erhverv Remote Attestation service.

After the check is complete (either planned, ad hoc, or prompted), the data is guaranteed to be unreadable while in motion. If the integrity check fails, it triggers a response from the TDC Erhverv SOC. While waiting for the integrity failure to be handled, it is possible to continue working in the application in a separate container (which has not failed its integrity check).



Contact us if you would like to know more.
If you have questions or you would like to know more; you are welcome to call us at **70 70 90 90** for a friendly talk about TDC Erhverv CloudKey® for Azure – Your answer to safeguarding cloud data

TDC Erhverv
Se fremad