BYTES Smarter together

www.bytes.co.uk/

ZERO TRUST | IN 2023

DATA

Protecting data is one of the primary responsibilities **of security and compliance teams**

Data should **remain protected** while at rest, in use, and when it leaves the endpoints, apps, infrastructure, and networks that are within the **control** of the organization.

To ensure protection and that **data access** is restricted to authorized users, data should be inventoried, classified, labelled, and, where appropriate, encrypted.

LEARN MORE

THE THREE CORE ELEMENTS OF A **DATA PROTECTION STRATEGY** ARE:

Know your data

If you don't know what sensitive data you have on-premises and in **cloud services**, you can't adequately protect it. You need to discover data across your **entire organization** and classify all data by sensitivity level.

Protect your data and prevent data loss

Sensitive data needs to be protected by **data protection** policies that label and encrypt data or block over-sharing. This ensures only a**uthorized users** are able to access the data, even when data travels outside of your corporate environment.

Monitor and remediate

You should continuously monitor sensitive data to detect policy violations and risky user behaviour. This allows you to take appropriate action, such as revoking access, blocking users, and refining your protection policies.

LEARN MORE

BYTES Smarter together

Tel: 01372 418 500
Click **here** to learn more about Bytes

ABOUT BYTES
Thanks to our passionate people, expert security consultancy and close vendor partnerships, we've helped hundreds of top brands transform, grow and adapt to the changing technology landscape.
And we don't plan on stopping anytime soon.