FUJITSU

# Compliance & Security


## Better to prevent than pay the price

Protect your organization – both from the threat of prosecution as well as being a victim of cyberattacks with our compliance and security strategy. Our extensive data ecosystem includes solutions for discovering, identifying, protecting, and recovering your data through its entire life cycle.

**The real threat**
While organizations strive to 'do more with less' it is important that they meet all legal and regulatory requirements, and also take effective measures to protect themselves from theft or hostile erasure of their intellectual property.

Legislators all over the world are constantly evolving regulations for various industries and activities. It is important to have fit-for-purpose tools to monitor and manage compliance to ensure they can meet requirements in different jurisdictions. The financial and criminal penalties for failure ensure it is a mandatory board-room topic and not something that can be left to chance.

Cyberattacks are increasingly threatening the success of organizations with ever-increasing sophistication and operating at industrial scale. The economic damage caused by cyberattacks has been growing rapidly, and every 11 seconds a business enterprise falls victim to a ransomware attack. Experts estimate that by 2031, ransomware attacks will occur every two seconds and annual damage will skyrocket from about $20 billion today to $250 billion.

> "39% of European organizations see security and compliance as the main challenge with regards to cloud operations."
>
> IDC European Multicloud Survey, September 2022

Since data is the heart of intelligent enterprises, a successful digital operation depends on the ability to develop a unified data management and protection architecture for modern multi-cloud infrastructures. As a digital enterprise, first and foremost, cybersecurity must be embedded at the core of your systems and processes and seen as a key business goal.

The traditional approach of securing only the infrastructure perimeter is no longer effective. Any infiltration must be contained, rather than gaining complete open access to everything inside the organization. A Zero-trust concept is a compelling strategy to reinforce defenses in a modern architecture – to reduce risk as application architectures evolve to micro-services.

# Do you want to discover any potential compliance and security risks in your environment?

The Fujitsu Security Consulting and Professional Services provides invaluable insight tailored to your particular organizational needs – and with a focus on protecting your business.

Fujitsu is uniquely positioned to help customers protect their hybrid cloud environments, because we can offer a wide range of solutions combining own technology with that of major software vendors. This enables us to provide you with unbiased advice to co-create an ideal solution that perfectly suits your organization's needs.

**To keep your hybrid cloud secure, we help you:**

- Effectively counter threats with a multi-layered approach to monitoring your data and providing early-warnings of unwanted activity.
- Build a zero-trust concept into your operations to resist attack propagation.
- Provide a data-driven ransomware strategy to help you strengthen your resilience against ransomware attacks and improve the security of your data – on-premises, in the cloud, or anywhere else.
- Continuously update your knowledge and awareness of emerging trends and threats and guide you on your journey toward a cyber-secure IT infrastructure and remain one step ahead.

**To keep your operations compliant in hybrid cloud, we help you:**

- Enable a data-driven strategy to help you understand and categorize your data. This will support your regulatory compliance and strengthen the security of your data – on-premises, in the cloud, or anywhere else.
- Implement data and storage solutions that help you understand what data you have as well as prepare you for cybercrimes like ransomware attacks.

## Fujitsu and ecosystem partner solutions to protect your hybrid cloud:

**NetApp Cloud Data Sense** – AI-driven technology to provide data governance across your entire estate enabling you to easily identify cost savings, compliance and privacy concerns, and optimization opportunities.

**Commvault® Data Governance** – provides a streamlined framework for risk management to define, find, manage, secure, and remediate sensitive data throughout hybrid cloud environments.

**VMware Carbon Black Cloud** – a solution that provides next-generation anti-virus, endpoint detection and response, advanced threat hunting, and vulnerability management within a single console.

**Commvault® eDiscovery & Compliance** – providing a fast, efficient and scalable data collection solution able to quickly collect electronically stored information.

**Commvault File Storage Optimization** – a storage management solution designed to drive storage efficiencies and manage data risks.

**Veritas Alta™** – a portfolio of cloud data services in a single, powerful platform, purpose-built for modern workloads, and engineered to achieve optimal security and performance.

→ Learn more