

Cybersecurity Solutions & data back-ups with Acronis - Service Design

VMotion provides consultative service design support for backup and cyber protection solutions using Acronis Cyber Protect. The service focuses on advising organisations on configuration options, design patterns, and best-practice use of Acronis capabilities to support resilience, security, and recoverability requirements. Services cover data protection, cybersecurity, disaster recovery, endpoint management, and automation considerations across hybrid and cloud environments.

Designed capability areas

Capability Area	Service Design Support
Data Protection	Advisory on backup approaches and protection models
Cybersecurity	Guidance on ransomware protection and malware prevention
Disaster Recovery	Advisory on recovery options and recovery objectives
Endpoint Management	Guidance on centralised management and patching options
Automation	Advisory on policy-based automation and efficiency features

Supported workload and platform scope

Workload Type	Examples
Endpoints	Windows, macOS, Linux
Servers	Windows Server, Linux Server
Virtualisation	VMware vSphere, Hyper-V, Nutanix, KVM
Cloud workloads	Azure VMs, Amazon EC2
SaaS platforms	Microsoft 365, Google Workspace
Applications	SQL Server, Exchange, SharePoint, Active Directory

Security framework alignment

NIST CSF Function	Service Design Guidance
Govern / Identify	Asset visibility and configuration awareness
Protect	Backup policies, immutable storage options
Detect	Behaviour-based threat detection guidance
Respond	Guidance on isolation and remediation workflows
Recover	Guidance on recovery options and validation

Scope of Service

This service provides consultative guidance to support the design and configuration of backup, cyber protection, and endpoint management solutions using Acronis. Scope includes requirements discussion, design recommendations, configuration guidance, and alignment to security and resilience objectives. Implementation, managed services, live incident response, and ongoing monitoring are excluded unless explicitly agreed.

Service Features

Feature	Description
Requirements discussion	Understanding backup, security, and recovery needs
Design guidance	Guidance on configuration and design options
Platform coverage guidance	Endpoints, servers, VMs, cloud, and SaaS
Ransomware protection guidance	Guidance on immutable storage and prevention
Disaster recovery guidance	Recovery objectives and recovery options
Automation guidance	Guidance on policy-based workflows
Governance alignment	Guidance aligned to recognised security frameworks
Documentation	Recommendations and guidance documentation

Service Benefits

Benefit	Description
Reduced configuration risk	Guidance helps avoid misconfiguration
Improved cyber resilience	Informed use of integrated protection features
Clear recovery understanding	Clarity on recovery options and limitations
Better decision-making	Independent, expert consultative advice
Faster implementation	Clear guidance accelerates deployment
Scalable approach	Guidance supports growth and change
Framework-aligned assurance	Alignment to recognised security frameworks

