Softcat

SECURE YOUR DATA

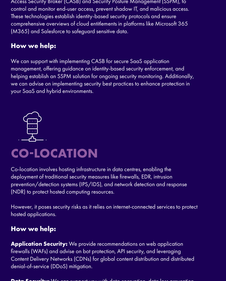
Securing your data is crucial to safeguard sensitive information according to regulations and maintain the trust of your customers and stakeholders.

Modern infrastructure and data governance practices are essential components of this as they can ensure that data is stored, transmitted, and processed with robust security measures. They provide the framework to mitigate cyber security risks, comply with regulations, and establish data resilience.

MODERN INFRASTRUCTURE

Your infrastructure is fundamental for data transmission, storage, and processing. It has advanced significantly to meet changing organisational needs, focusing on modern technology for enhanced data management.

The design, deployment, and maintenance of modern infrastructure directly impacts security, making it a critical component in safeguarding sensitive information against cyber threats and breaches.



PUBLIC CLOUD MIGRATION AND MODERNISATION

Data security risks in public cloud migration and modernisation involve misconceptions about the cloud responsibility model, an expanded attack surface, and challenges with serverless security. A lack of comprehensive security observability tools can hinder effective threat response.

How we help:

To enhance data security during public cloud migration and modernisation, we would begin by clarifying the Cloud Service Provider's (CSP's) responsibility model, helping you understand your security obligations. We can also manage attack surfaces, improve software supply chain security, and strengthen serverless and container environments.

For ongoing security, we use observability tools to proactively audit and analyse your cloud posture, ensuring quick threat detection and response.

ON-PREMISE AND PRIVATE CLOUD

Depending on your industry, on-premise infrastructure might be necessary for specific applications and data governance, utilising technologies like Zero Trust Network Access (ZTNA) and Server-Side Encryption for enhanced security.

Both on-premise and private cloud environments require strong data security measures, including micro-segmentation (firewalls) and micro-segmentation (workload-based), to prevent unauthorised access and data breaches. Additionally, Next-Generation Endpoint Detection and Response (NG-EDR) scanning of storage is essential for compliance and improved data security.

How we help:

We can support you by assessing your current infrastructure to optimise security, assisting in technology selection, developing a precise ZTNA solution for adaptable access control, implementing Secure Services Edge (SSE) for enhanced remote security, and establishing strong security measures, including Firewall segmentation, to safeguard your data.

SaaS/HYBRID

SaaS and hybrid environments rely on robust data security measures, like Cloud Access Security Broker (CASB) and Security Posture Management (SSPM), to control and monitor end-user access, prevent shadow IT, and malicious access. These technologies establish identity-based security protocols and ensure comprehensive overviews of cloud environments in platforms like Microsoft 365 (M365) and Salesforce to safeguard sensitive data.

How we help:

We can support with implementing CASB for secure SaaS application management, offering guidance on identity-based security enforcement, and helping establish an SSPM solution for ongoing security monitoring. Additionally, we can advise on implementing security best practices to enhance protection in your SaaS and hybrid environments.

CO-LOCATION

Co-location involves hosting infrastructure in data centres, enabling the deployment of traditional security measures like firewalls, EDR, intrusion prevention/detection systems (IPS/IDS), and network detection and response (NDR) to protect hosted computing resources.

However, it poses security risks as it relies on internet-connected services to protect hosted applications.

How we help:

Application Security: We provide recommendations on web application firewalls (WAFs) and advise on bot protection, API security, and leveraging Content Delivery Networks (CDNs) for global content distribution and distributed denial-of-service (DDoS) mitigation.

Data Security: We can support you with data encryption, data loss prevention (DLP), data masking for sensitive information, data access controls to limit unauthorised access, and solutions for secrets management.

RELATED SOFTCAT SERVICES

- **Cyber Resilience Assessment** - Employs focussed frameworks for those seeking initial cyber security insights or those who find larger frameworks unnecessary. It delivers a detailed overview and report with key findings and recommendations.
- **Microsoft 365 Security Assessment** - Audits your Microsoft 365 and Office 365 environments against industry security benchmarks and provides recommendations to maintain secure practices.
- **Managed SIEM Service** - Monitors for and detects security threats across various IT, cloud and SaaS environments, utilising advanced threat intelligence and offering expert guidance for rapid response.
- **Security Baseline Assessment** - Offers a comprehensive analysis of your cyber security posture against industry best practices to identify vulnerabilities, assess risk profiles, and provide actionable steps for improving your data security.

DATA GOVERNANCE

Data governance plays a crucial role in data security by establishing a framework to manage and safeguard sensitive information.

It outlines responsibilities, processes, and access control to maintain data integrity and availability while enabling efficient recovery.

Additionally, it enforces data classification, retention, and encryption policies to enhance data security defences.

DATA RESILIENCE

Data resilience in data security, including cyber incident response, recovery setups, and ongoing resilience testing, is vital. Governance practices oversee the data lifecycle, encompassing privilege management, stewardship, data handling, loss prevention, and audit trails. Whilst metadata management organises data origin, usage, and context.

How we help:

We enhance your data resilience by simplifying data discovery through detailed reports that reveal data location and flow within your organisation. This empowers you to make informed decisions to fortify your data and ensure compliance.

We also assist you in understanding and meeting regulatory requirements specific to your industry, providing expert support in managing policies, procedures, standards, and records for a robust foundation in security management.

BACKUP

Backup is crucial for data security, enabling data non-repudiation and ensuring accessible backups to verify information integrity and source.

Compliance with regulations like GDPR, CAF, NIST CSF, and NIS2 depends on proper data sovereignty and retention to meet legal requirements and safeguard sensitive data. So, reliable backups are essential for quick recovery in the event of data breaches or losses.

How we help:

That's why we offer a fully managed backup service tailored to your needs, whether you prefer a third-party data centre or cloud-based backup. Our services enable faster recovery, reduced expose, and enhanced data security.

RECOVERABILITY

Immutable backups with an audit trail and air-gapped storage are crucial defences against ransomware attacks and data loss. Data immutability, including directory services, is essential for successful recovery; without it, data restoration becomes significantly less likely.

A clean environment is crucial for business continuity and disaster recovery (BCDR), requiring a comprehensive approach for swift recovery. Operational resilience now includes BCDR as a company-wide element, primarily due to cyber threats.

How we help:

Softcat can conduct cyber resiliency assessments based on NCSC standards and assist you in navigating other regulations, such as the Digital Operational Resilience Act (DORA).

We can enhance data security and recoverability with a tailored disaster recovery solution. Our team can work closely with you to ensure continuous replication of critical workloads from VMware or Hyper-V to a secure secondary site. Additionally, we provide ongoing management and support for your disaster recovery site's firewall, replication monitoring, and proactive issue resolution.

ARTIFICIAL INTELLIGENCE

The use and value of AI tools are rapidly evolving, and the first key goal for maximising their benefits is to focus on data.

Data needs to be collected, cleaned, and managed properly to ensure that AI operates efficiently and safely. This is crucial not only for in-house AI development but also for commercial AI adoption, especially in light of regulations like the EU AI Act and the need to understand the controls that can be applied to AI adoption.

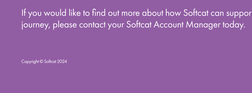
How we help:

Softcat can provide you with guidance, assessments, and assistance in setting up practical AI governance frameworks, threat modelling, and selecting and implementing controls to secure AI.

RELATED SOFTCAT SERVICES

- **Orisium Data Assessment Service** - Provides valuable insights into your data and assists with risk mitigation by enhancing data access control and ensuring data compliance.
- **Governance, Risk and Compliance Assessment Service** - Helps you manage your data to meet regulatory obligations, address key risks, and ensure your information security strategy is aligned with your business objectives.

WHY SOFTCAT?



Some of the reasons our customers choose to partner with Softcat in their cyber security efforts include:

Expertise – With decades of combined experience in engineering, technical, security operations, executive leadership, governance, and development security, our team comes from diverse backgrounds, including the armed forces, healthcare, central government, financial services, managed security service providers, manufacturing, and more. We deeply understand customer needs and partner objectives at a highly detailed level.

Customer experience – We take a customer-led approach. We understand that your security needs are unique, and we're here to listen and provide customised support to ensure you get the best protection possible.

Empathy – With a diverse team boasting extensive backgrounds and expertise in various aspects of cyber security, including breach management, auditing, recovery, and more, we approach your cyber concerns with empathy and a strong commitment deeply ingrained in our company culture.

Actionable data and insights – Softcat dedicates various business functions to collaborating with vendors and partners, optimising our market approach. The combination of our broad array of customers, our partnerships among major security vendors worldwide and our enduring customer relationships means we excel in providing unparalleled product analysis and market trend insights.

PARTNER ECOSYSTEM

Within our ecosystem of trusted vendors and partners, we've fostered strong relationships. These connections empower us to access the most fitting, best-in-class expertise and solutions to safeguard your organisation.

Cisco Partner · Microsoft · paloalto NETWORKS · mimecast · CROWDSTRIKE · SOPHOS · RAPID7 · tenable · FORTINET · TREND MICRO

TAKE THE NEXT STEP

If you would like to find out more about how Softcat can support you on your cyber security journey, please contact your Softcat Account Manager today.

Softcat