



# **CONTROL IN THE CLOUD**

## **Cloud-native data security**

Extending your visibility and control to the cloud, while retaining control over the data and user activity in unsanctioned and sanctioned cloud services.



**Control:** Enhancing controls within cloud services using remediation actions that are specific to cloud and relevant to the cloud context, data and connections.



**Framework:** A three-part framework – identify, control, and protect – is used with a unified policy framework across all cloud services with remediation.



**Capabilities:** Protecting information in the cloud using security controls that are applied to data in the cloud, including data loss prevention, identity and access management, encryption, and user and entity behaviour analysis.



**Purpose-built data security:** Addressing the unique scale and security challenges of cloud computing, while maintaining performance and delivering an excellent user experience.

## Introduction

The ability to protect business-critical data is essential in today's digital economy. High-profile data breaches have disrupted operations and impacted financial performance at enterprises worldwide, making information protection a C-level and board-level concern. Datacentrix offers a cloud-native data compliance and security solution that delivers a complete set of capabilities to protect data wherever it lives in the cloud.

## Today's security stack

Corporate data has, until recently, been primarily stored in applications, computers, and databases on corporate networks or on managed computers within the perimeter. Today, IT professionals treat data differently depending on its location, resulting in a security approach that focuses on two objectives:

- 1. Managing information in trusted repositories within the perimeter.** Here, companies use a variety of security technologies, including data classification, encryption, and user and entity behaviour analytics (UEBA).
- 2. Preventing sensitive information from leaving the perimeter.** Many companies have invested in data loss prevention (DLP) solutions that involve enforcing policies.

## The perimeter is disappearing

The rise of cloud computing and bring-your-own device (BYOD) has steadily eroded the perimeter to the point that business-critical information now lives in many places outside of the corporate network and managed devices.

## Cloud-native data security

Datacentrix delivers cloud-native data compliance, visibility and security, a set of capabilities that protects information in today's cloud-first technology landscape.

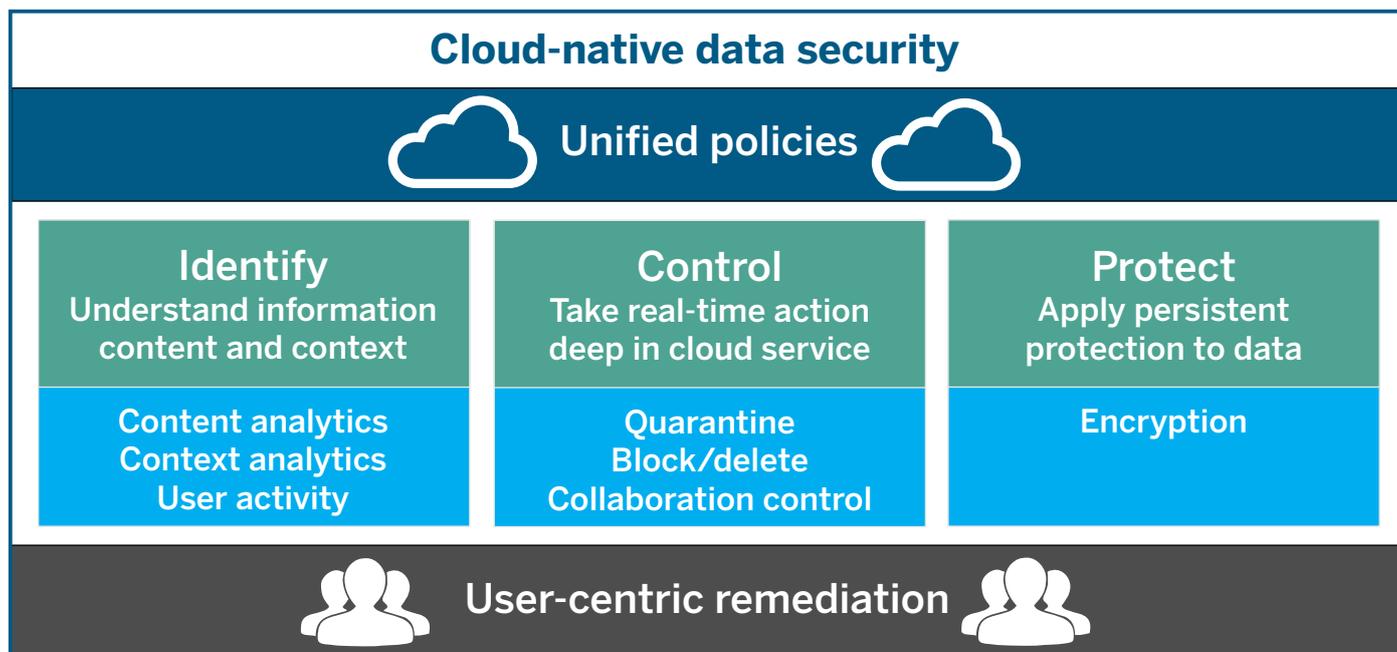
The solution extends familiar security concepts from the client-server era and reimagines them as applied to data in the cloud, including:

- Identity and access management;
- User and entity behaviour analysis;
- Encryption; and
- Data loss prevention.

The solution layers in controls for the security challenges that enterprises face as corporate data moves to the cloud, delivering complete visibility and control over your data and user activity in cloud services, both sanctioned and unsanctioned (ShadowIT).

## How it works

Cloud-native data visibility, control and security is aware of cloud context, data, and connections. The solution enforces controls within cloud services using remediation actions specific to cloud. The approach uses a three-part framework: Identify, Control, and Protect with a unified policy framework across all cloud services and remediation that places the user at the centre.



## Identify

**Content analytics:** The platform's content engine leverages a complete set of analysis tools to identify information and catalogue it automatically to enforce content-specific policies. The system leverages keywords, standard and custom data patterns, document and database fingerprints, document metadata, and detected file types. The policy engine supports Boolean logic, proximity match, exact match, and similarity match, allowing enterprises to craft targeted policies.

**Context analytics:** The context of your information is also identified in the cloud. This includes access permissions on files and folders extended to the entire company, specified users internally or externally, anyone with a link, or files open to the Internet along with the level of access.

**User activity:** The solution assesses user activity, normalising all user actions into common activity types across cloud services and building robust data models of normal user behaviour based on the user's role for each cloud service, and leverages UEBA to detect unusual behaviour patterns that indicate active account compromise and malicious internal users.

## Control

Datacentrix integrates directly with cloud services, enforcing real-time controls over how information is accessed, manipulated, and shared within these services.

**Quarantine:** The solution allows enterprises to define multiple levels of incident severity based on cloud content, context, and activity, and enforces distinct response actions based on the severity of the incident. The control capabilities include the ability to quarantine data within an administrative account in the cloud service where it was found.

**Block/delete:** The solution can also remove data from cloud services to comply with regulatory requirements and neutralise malware. Based on cloud context, Datacentrix can modify access rights to downgrade file or folder permissions, remove permissions for a user entirely, and revoke shared links.

**Collaboration control:** The solution enforces activity-level controls.

## Protect

**Encryption:** Datacentrix applies protection to your information that persists wherever it goes inside the cloud or outside the cloud. Datacentrix encrypts information using enterprise-controlled encryption keys, making your information inaccessible to unauthorised third parties while preserving application functions like format and end-user functions such as search.

## Unique policies

Underlying Datacentrix' data security capabilities is a unified set of policies that applies to all your information in all your cloud services.

**Policy import:** Cloud-native data security supports the import of policies from legacy on-premises security solutions and provides numerous out-of-the-box policy templates.

**Policy creation:** The solution supports rich policy creation capabilities using a wide range of rules and response actions that span the identify, control, and protect capabilities.

**Response action:** The solution allows you to combine cloud content, context, and behaviour rules with Boolean logic to establish what triggers a response action. These response actions can include taking real-time action to control data and activity within cloud services, and applying persistent protection to data in the form of encryption.

## User-centric remediation

Autonomous remediation works directly with end users to resolve incidents, allowing security analysts to focus on the most critical ones. When an end user violates a policy, they receive a coaching alert that, where possible, occurs natively within the cloud service. This automation allows end users to resolve 97% of incidents on their own, reducing the average security analyst's monthly cloud incident workload from 387 to 12.



**With Datacentrix, enterprises have total authority over their data and user activities anywhere in the cloud, ensuring information is protected and compliant so you can confidently unleash the power of the cloud to accelerate your business.**

## Built in the cloud, for the cloud

By delivering a purpose-built cloud-native data security solution, Datacentrix is able to address all of the unique scale and security challenges of the cloud, while maintaining the performance and user experience that employees are accustomed to when using cloud services. Different deployment modes cover all cloud visibility and security use cases.

## Summary

Corporate data is rapidly moving beyond the reach of your existing security stack. Datacentrix extends visibility and control to the cloud, while retaining complete command over the data and user activity in cloud services. The solution empowers enterprises to identify their data and understand user activities in the cloud, take action to control their data and user activities, and apply persistent protection to their data across all cloud services.

### Get an audit of your cloud usage

Datacentrix provides a personalised assessment of cloud usage in your organisation. We'll deliver a report summarising:

- All cloud applications in use;
- High-risk apps accessed by your employees;
- Gaps in your proxy/firewall policy enforcement; and
- Redundant services used in each category.



**Giving business access to class-leading computing that is secure and affordable. Journey with Datacentrix to the cloud.**



**+ 27 87 741 5000**



**sales@dcxcloud.co.za**



**www.datacentrix.co.za**