

# SAFEGUARD CRITICAL IBM i DATA WITH PRECISION AND RESILIENCE, USING MAXAVA SECURITY

## Maxava Security

In today's digital landscape, the reliable and stable IBM i server is often classed as the cornerstone for countless organizations, housing key applications and mission-critical data. However, with evolving threats such as malware, ransomware, and insider attacks, proactive protection is paramount. Introducing Maxava Security, a cutting-edge solution designed to safeguard your IBM i data and help to maintain business continuity.

## Business Benefits

### Enhanced Security

Maxava Security provides a proactive approach to data protection, minimizing the risk of data breaches and unauthorized alterations.

### Business Continuity

Ensure uninterrupted operations with rapid recovery capabilities, reducing downtime and mitigating financial losses.

### Data Integrity

Preserve the integrity of critical data with automated archiving and secure storage, safeguarding against both intentional and unintentional harm.

### Cost Savings

By preventing data loss and minimizing downtime, Maxava Security can help organizations avoid costly repercussions associated with security breaches and operational disruptions.

## Features

### Granular Access Control

- Define and enforce rules dictating authorized users for specific files.
- Mitigate the risk of unauthorized alterations by limiting access to trusted personnel and processes.

### Automated Archiving

- Constantly monitors and preserves point-in-time copies of critical data before unauthorized changes.
- Objects identified by access control rules are promptly duplicated, encrypted, and stored.

### Flexible Storage Options

- Secure archive repository can reside locally, in a co-location facility, or in the cloud.
- Offers flexibility and scalability to meet diverse storage needs.

### Rapid Recovery

- Agile recovery of archived objects in the event of corruption, malware assaults, or ransomware incidents.
- Ensures quick bounce-back from unforeseen incidents without compromising data integrity.

## Setup in 3 Easy Steps

- Define your critical data.
- Decide who is authorized to change it.
- Be alerted to exceptions coupled with a checkpoint recovery point.