

Mi7 Security Reports, monitors and alerts to changes made to security on the IBM i

WHAT Mi7™ SECURITY DOES FOR YOU

Mi7 Security stores historical records of security changes made on your system. Ability to create custom reports & compliance reporting and alerting for your IBM i.

Maxava provides a cloud-based graphical interface accessible from all devices. Built on the same proven innovative technology used for our Mi8 monitoring platform.

IBM i Security Event Categories

Allow you to monitor the IBM i, for:

- ✓ System Values
- ✓ Network Attributes
- ✓ User Profiles
- ✓ Object Authorities (including the IFS)
- ✓ Adopted program authorities
- ✓ Exit point programs

Mi7 Allows you to define multiple compliance policies to enable IT and external auditors. The cloud console can be configured to receive alert to indicate when non-compliance items are found.

Mi7 also allows you to define rules to real-time check to the ibm security journal and history log for potential security issues.

Exit Point Monitoring

Mi7 can report on access obtained via the IBM i exit points. Rules can be defined to monitor the more critical accesses and alert through the Cloud Console. Mi7 will also monitor and advise if someone removes a required program from an exit point.

Why Choose Mi7

- ✓ Mi7 helps an organisation ensure that their IBM i Security Event Categories being monitored have only changed when expected and alerts you when unintentional or malicious changes have been made or attempted.
- ✓ Mi7 provides an easy and reliable solution to allow the security monitoring and reporting of IBM i systems situated in one or multiple locations.
- ✓ Mi7 allows easy and straight forward compliance reporting for internal and external requirements.
- ✓ Mi7 assists you to ensure your systems are correctly secured.

For your trial request, visit maxava.com/security-mi7-trial-request

