SERVICES BUNDLE

IDENTITY & PRIVILEGED ACCESS MANAGEMENT

ADD AN EXTRA LAYER OF SECURITY TO YOUR IBM i ENVIRONMENT

The majority of data breaches start with abuse of access credentials that could have been averted.

Every user on an IBM i system has a user profile - sometimes multiple profiles. Users may also have several profiles across multiple systems, each used for different job functions. Multiply that by the size of the data centre and it becomes difficult to stay in control.

Elevated privileges compound the challenge. Privileged accounts are necessary for effective IT environments, they can't be avoided, but they must be managed.

Enforcing the principle of least privilege helps prevent the spread of malware, decreases your cyber-attack surface, improves workforce productivity, and helps demonstrate compliance.

Get a free! non-disruptive security scan today.

TRUSTED TECHNOLOGY PARTNERS

FORTRA™ IBM i IBM Platinum Partner

IDENTITY AND PRIVILEGE ACCESS MANAGEMENT OVERVIEW

Reduce risk with consistent management of user profiles highlighting policy exceptions and unauthorised.

WHY PRIVILEGED ACCOUNTS GO UNMANAGED

- Overworked admins attempt to improve user productivity by granting too much access
- Privilege creep when users change roles but keep their elevated status
- Zombie accounts when users leave the organisation, but credentials are not disabled
- Unchanged defaults for all-powerful service accounts
- Password sharing across multiple systems
- Lack of monitoring – you can't fix what you can't see

PRINCIPLE OF LEAST PRIVILEGE

- Restricting account creation and permission levels to the exact resources a person or system needs to fulfil a defined role
- Managing access privileges increases security by reducing user error and malicious attacks
- Consistent admin approach to access improves operational efficiency
- Privileged activity monitoring simplifies auditing and compliance requirements
- Privilege access management must be extended to cloud environments and applications

GROW SAVE INNOVATE PROTECT

IDENTITY & PRIVILEGED ACCESS MANAGEMENT BUNDLE

Here's what to expect from this cutting-edge IAM/PAM bundle to secure IBM i systems.

INSIDE THIS BUNDLE:

IDENTITY MANAGEMENT

Central administration to create and change user profiles across multiple systems.

- Simplify user profile management
- Accelerate onboarding new users
- Maintain compliance

PRIVILEGED ACCESS

Ensure special authorities are granted only to those who need them, when they need them.

- Protect sensitive IBM i Information
- Control user privileges
- Capture IBM i user activity
- Save time and resources

MULTI-FACTOR AUTHENTICATION

Configure MFA and import users from Active Directory.

- Comply with security standards
- Enforce risk-driven security policies
- Protect access from any device and location

PASSWORD SELF HELP

Reduce the cost of password issue and increase user productivity.

- Secure self-service password resets
- Set a strong password policy
- Maintain an audit trail

COMPLIANCE REPORTING

Manually verifying that security policies are being followed can be overwhelming.

- Simplified IBM i configuration reporting
- Report customisation
- Automated reports provide evidence.

FIND OUT MORE...

Your IBM i environment can be secure, but that means rooting out system vulnerabilities and establishing robust security controls.

Speak with a CSI expert today to find out more about IBM i security.

CSI Ltd Head Office

CSI House
2940 Trident Court
Birmingham Business Park
Solihull Parkway
Birmingham B37 7YN

CONTACT INFO

+44 (0) 800 1088301
info@csiltd.co.uk
www.csiltd.co.uk