FORTRA

Fortra's Tripwire Enterprise and IBM i

Many of the world's largest companies rely on IBM i operating on IBM Power Servers as their strategic platform for business-critical activities such as retail, distribution, logistics, banking, manufacturing planning, healthcare, insurance, hospitality management, government administration, and legal case management. Given the widespread use of the IBM i operating system, advanced cybersecurity solutions are essential to protect organizations from targeted cyberattacks.

Tripwire® Enterprise continuously monitors for suspicious changes that could indicate compromise while automating the arduous work of regulatory compliance, giving you a complete integrity management and compliance solution that covers not only platforms like IBM i, but your entire infrastructure including files, databases, servers, endpoints, ephemeral assets, and even industrial OT environments.

What Is Tripwire Enterprise?

Tripwire Enterprise is the leading compliance monitoring solution, using file integrity monitoring (FIM) and security configuration management (SCM). Backed by decades of experience, it's capable of advanced use cases unmatched by other solutions. This fully integrated suite of solutions for policy compliance, system integrity, and remediation management reaches far beyond simple compliance. It enables teams to rapidly achieve an increased level of security across the entire enterprise.

Tripwire Monitors IBM i Integrity

Tripwire Enterprise can be configured for IBM i using a Secure Shell (SSH) connection. This connection is configurable for public-key encryption to secure the commands while in transit across the network. While the majority of nodes created within Tripwire Enterprise are based on the Tripwire Axon® agent, the IBM i solution runs via a Tripwire Enterprise Network Device.

The Tripwire Enterprise Network Device and SSH connection directly link to the IBM i's Portable Application Solutions Environment (PASE for i), which offers an AIX shell for command execution. This approach doesn't require code installations and provides scalability while decreasing the need for IBM i administrator oversight.

FORTRA AND IBM i

Fortra is your ally in IBM i cybersecurity. In addition to the integrity management enforcement provided by Tripwire Enterprise, additional Fortra solutions give you complete control over your IBM i platform.

- Antivirus/Ransomware
- Command Security
- Database Change Monitor
- Exit Point Manager
- Multi-Factor Authentication
- Password Self Reset
- Authority Broker Privilege Access
- Regulation Compliance Reporting
- Secure File Transfer
- Security Policy Enforcement
- IBM i Auditor
- SIEM Agent Integration
- User Profile Manager
- Security Review/Risk Assessment
- Free Security Scan
- SSO Services
- Managed Security Services

The PASE shell can then run IBM i OS system commands and direct information to the Tripwire Enterprise console using Command Output Validation Rules (COVRs). When these COVRs are run, they provide you with point-in-time snapshots of your IBM i instance and compare the results to earlier runs to identify noteworthy changes in objects, attributes, and configuration settings, including:

APPN Attributes	Trigger Programs
IPL Attributes	Controller Descriptions
Reply List Entries	Network Attributes
Active Profile Lists	User Profile Group Members
Libraries (User/Application)	Device Descriptions
Security Attributes	Objects owned by QDFTOWN
Adopted Program Authority	User Profiles
Libraries with PUBLIC Auth	Edit Descriptions
Security Audit Attributes	OS Version
Authorization Lists	Users with *SPLCTL (Special Auth)
Job Descriptions	Firmware Status
Software Resources	PTFs
Authorized Users	IBM Supplied Users (Q*)
Journal Attributes	Function Usage
Subsystem Descriptions	Registry Exit Points
Configuration Lists	Users with default passwords
License Key Info	Hardware Resources
System Values	Relational DB Entries
Connection Lists	SSHD Configuration
Line Descriptions	

Superior Security: Continuous Integrity Management

Through this connection, Tripwire Enterprise can continuously monitor IBM i systems for unauthorized and suspicious changes against a known and secure baseline state. It then guides you through rapid remediation and provides root cause drill-down to investigate the nature of significant changes.

Continuous Compliance: Automate PCI DSS and More

In addition to the security benefits of using Tripwire Enterprise to monitor IBM i systems, this process can also greatly simplify the enforcement of regulatory compliance by enforcing built-in policies for all major compliance mandates and best practice frameworks.

With a growing library of over 4,000 platform and policy combinations, Tripwire helps organizations achieve and maintain compliance with standards like NERC CIP, HIPAA, GDPR, and many others. You can even create your own custom internal compliance policies to ensure your environment is tuned exactly as it should be.

Operational Efficiency: Support for the Whole Environment

When you use Tripwire to manage the integrity of your digital environment, you can trust in one system of truth and reporting for not only IBM i but for your entire environment. Tripwire extends to cover your organization's environment without leaving gaps that could impede compliance or compromise security.

How to Get Started With Tripwire for IBM i

Once you have your Tripwire Enterprise instance up and running, the Tripwire Services Team will assist you in setting up your IBM i configuration via a standard professional services engagement or Tripwire Advisory Services, the subscription-based, remote professional service that pairs you with a professional services consultant for a year of ongoing sessions. Contact us today at tripwire.com/contact.

FORTRA®

Fortra.com