Detect and Remediate Changes that Threaten Compliance

MANAGED SECURITY

File Integrity Monitoring

Closing a Critical Security Gap

Changes to configurations, files and file attributes throughout the IT infrastructure are just part of everyday life in today's enterprise organizations. To protect critical systems and data, you need to detect all changes, capture details about each instance, and use those details to determine if a change introduces security risk or non-compliance. You also have to do that in real-time to stop an attack from succeeding — or minimize the impact of a successful one.

Reduce Your Workload

Most IT organizations have too much to do and not enough time or staff to do it. Automation is essential to keep up with the workload. DataBank leverages automation to detect all changes and remediate those that take a configuration out of policy. At the same time, intelligent change management auto-promotes countless business-as-usual changes, so IT has more time to investigate changes that introduce risk and impact security.

At-A-Glance

- Helps meet compliance requirements such as FedRAMP, HIPAA/HITECH, and PCI-DSS through policy management and continuous configuration assessment
- Creates an approved baseline to validate approved changes against
- Correlate alerts, events, and incidents from various sources to detect suspicious activity
- Provides an audit trail of all suspicious findings
- Provides a historical perspective of your entire security and compliance operation

GET A QUOTE

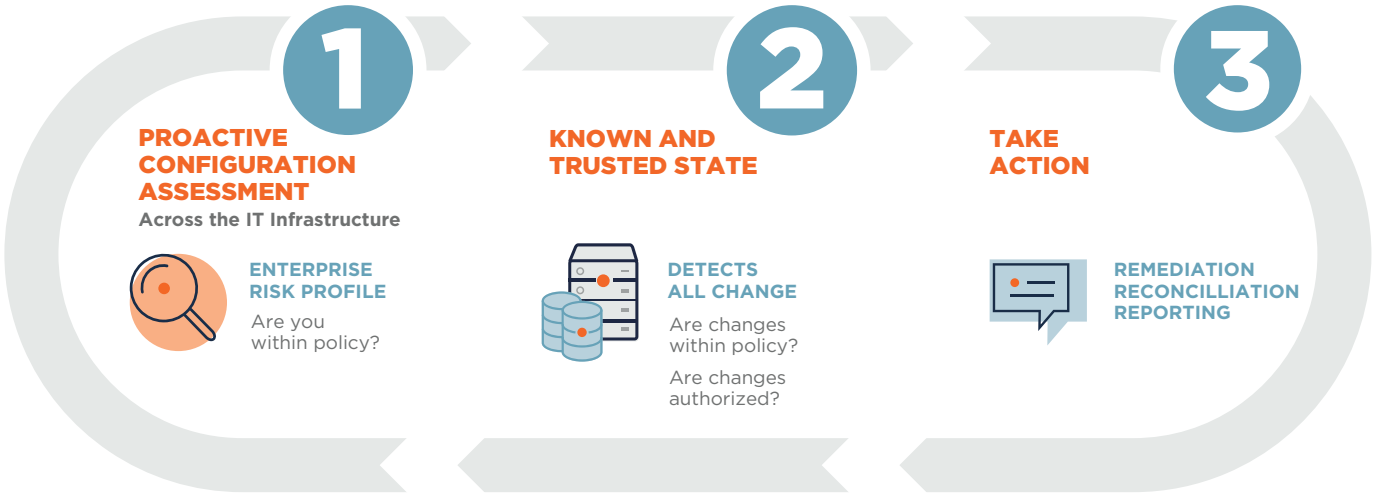
Discover the DataBank Difference

ask@databank.com | 800.840.7533

DATABANK
Data Center Evolved™

MANAGED SECURITY

File Integrity Monitoring



Features

- Compliance enablement for FedRAMP, HIPAA/HITECH, and PCI-DSS
- Real-Time Change Intelligence
- Real-Time Change Detection
- Automated Alerts
- Automation of large batches of changes, such as when operating system or application patches are pushed

Benefits

- Helps meet up to 80% of compliance requirements including wavier exception management with thresholds and severities
- Resolves issues before they result in a significant data breach, audit finding, or long-term outage
- Determines if immediate attention is required to safeguard against exploits, and ensures your configurations are continually compliant
- Ensures exposures are remediated immediately and no exposure goes undetected
- Unburdens your IT staff from the day-to-day manual intervention required to keep pace

TALK TO AN EXPERT

Discover the DataBank Difference

ask@databank.com | 800.840.7533

DATABANK
Data Center Evolved™