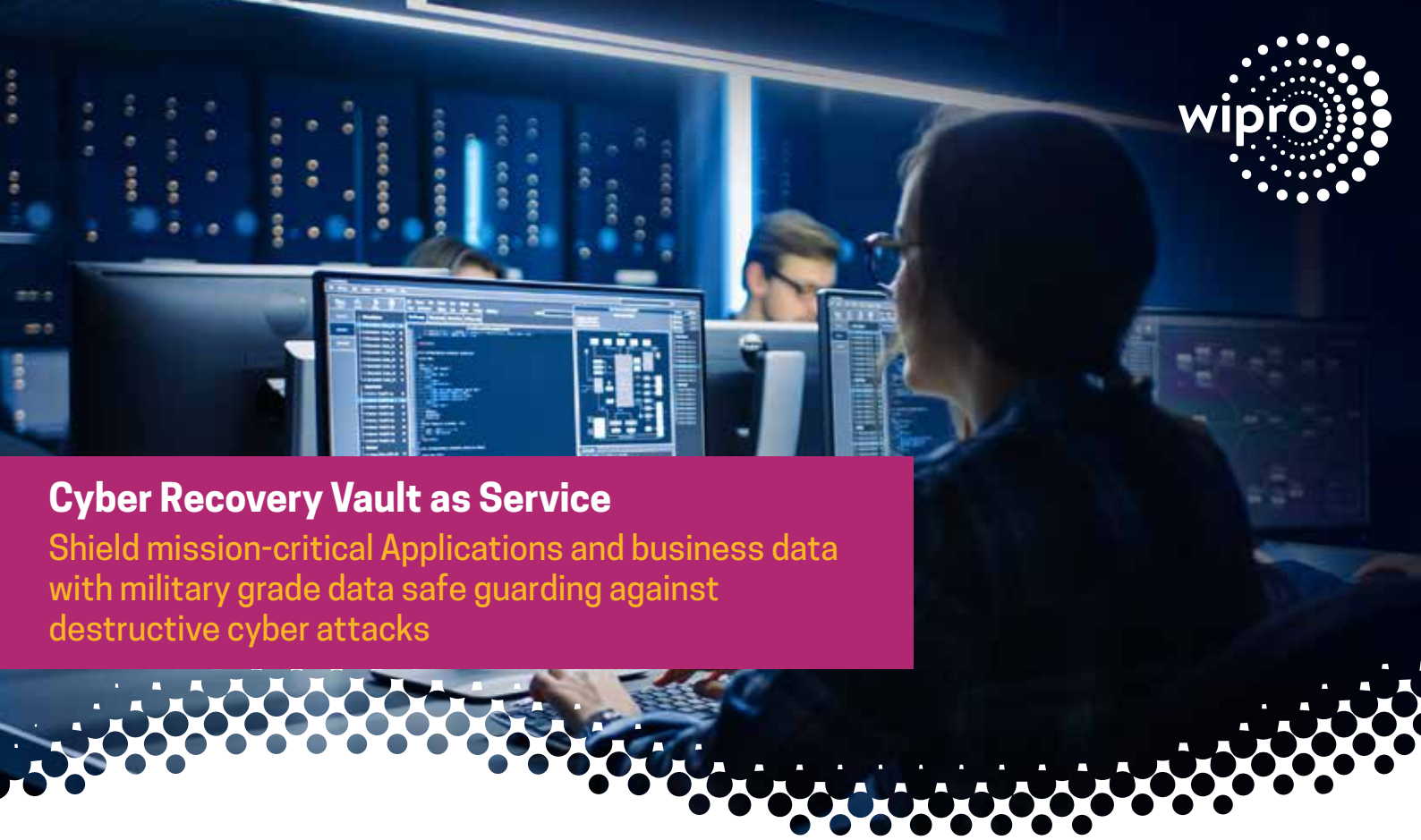

Cyber Recovery Vault as Service

Shield mission-critical Applications and business data with military grade data safe guarding against destructive cyber attacks

Introduction

Wipro's Cyber Recovery Vault as a Service automates end-to-end workflows to shield critical data, identify suspicious activity and perform data recovery when required. It is a comprehensive and holistic service featuring a multi-layered approach to protect backup data against ransomware, detect and rapidly recover from an attack.

Key Takeaways

- Detect anomalies that signal potential attacks leveraging real time machine learning insights
- Deep visibility to ensure that backups are clean and will not re-inject vulnerabilities while restoring
- Integrate with Wipro's Service Theatre for single dashboard and workflow automation delivering autonomous actions

Protect backup data with unique immutable architecture and automated air gap with data isolation and governance

Key Benefits

Faster and easier recoveries

- Fully secured and automated recovery from infected data in the event of a cyber-attack, an insider threat or a rogue admin
- Reduces business risk and time spent on ransomware remediation

Native immutability to safeguard backups

- Ensures backups are not compromised by ransomware
- Eliminates operational and financial complexity associated with isolated recovery

Minimize Recovery point objective (RPO) impact with granular visibility

- Quickly identifies which applications and files were impacted and where to
- Eliminates manual assessments, such as scanning through millions of files to
- Minimizes risk of data loss associated with mass restores that include

Established people and technology process

- As part of the service, Wipro deploy task force with established process to deliver the activities for proactive protection and secured recoveries with enterprise approved process

Features

Isolated secure vault - It hosts organization critical data in an isolated vault, which is air gapped, offline and in a secured environment.

Detection - Provides a secure and powerful solution to combat malware, ransomware and other cyber-attacks. Detects encryption, deletion and other changes in protected workload.

Analytics - Uses machine learning to analyze content-based statistics and finds corruption. It also provides a forensic report for further diagnosis. The machine learning algorithms have been trained by all the latest trojans and ransomware and can be updated as new attack vectors are discovered.

Cyber Management - Monitors the integrity of the data and sends alerts when changes occur that are indicative of a cyber-attack. This added layer of security is designed to compensate for when attacks circumvent existing security defenses. discovered.

Automation - Wipro's FluidIT Service Theatre integrated with the cyber recovery solution can provide a single pane of dashboard and workflow automation to take actions based on set of rules and policies.

Aligned with NIST cyber security framework, the cyber recovery solution framework enables organizations to evolve their recovery and business continuity strategies in addition to focusing on threat detection and remediation.

Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,
India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful.

A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 180,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/TBS/ MAY-DEC 2020