



Wipro Cyber Recovery Vault Solutions Powered by Dell Technologies

**Protect your critical data
information assets
effectively to withstand and
recover from adversity
arising from cyber space,
powered by analytics,
machine learning and
forensic tools.**





Solution

Cyber Attack – The enemy of today’s data driven economy

Cybercrime, ransomware attacks, hacking—not a day passes without technology crimes making the news. The threat actors’ motives go beyond wrecking corporate reputations, financial loss, penalization from regulators whilst hurting customer and employee trust. Ransomware, in particular, is widespread, and its frequency is accelerating. Additionally, there seems to be no limit to the creativity of the cyber criminals launching these attacks which are instigated across all the industry sectors.

Cyber-attacks take many forms and the attackers may have a variety of motivations, but the target of their efforts is consistent: destroy, steal and ransom valuable digital data for financial gain, social or political purposes. The tactics and technologies used in cyber-attacks continue to evolve rapidly, which makes preventing an attack nearly impossible. The most difficult type of cyber-attack to defend against is the ‘insider’ attack. By obtaining valid credentials such as usernames and passwords, an attacker can pose as an authorized user and wreak havoc.

Wipro and Dell Technologies join together to help customers battle cyber war

The impact of being unable to recover critical data and resume business operations after an attack can be devastating. Avoiding ransomware is of utmost importance to the CIO and CISO. Wipro and Dell Technologies jointly developed the cyber recovery reference architecture to protect enterprise critical data assets their crown jewel to provide:

- Automated air gap with data isolation and governance
- CyberSense analytics and machine learning to monitor data integrity
- Forensic tools to discover, diagnose and remediate ongoing attacks
- Integration with Wipro Service Theatre for single dashboard and workflow automation
- Automated non-invasive deployment blue print enabled with Wipro ASPIRE

● 69% of IT Decision makers lack confidence that they could reliably recover all business-critical data in the event of a cyber attack

-Global data protection index survey 2020 Snapshot

- Protects your organization’s most critical data within an isolated secure vault
- Creates isolated gold copies in a secure vault which can be restored post identification of ransom attack

Protecting your business starts with protecting the Crown Jewels

PROTECT:

Business-critical data from ransomware and cyber-attack related incidences resulting in data corruption

IDENTIFY:

Intelligence to sense data corruption with machine learning and analytics

ACCELERATE:

Recovery of 'known good' data to quickly resume business operations

Wipro and Dell Technologies Cyber Resiliency Solution

Aligned with the NIST Cybersecurity Framework, the Cyber Recovery solution enables organizations to evolve their recovery and business continuity strategies in addition to focusing on threat detection and remediation.

Isolated secure vault - It hosts organization critical data on Dell infrastructure, and is air gapped, offline and in a secured site with physical and environmental security

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

Analytics - Uses machine learning to analyze over 100 content-based statistics and finds corruption with up to 99.5% confidence. 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 defense

Automation – Wipro's FluidIT Service Theatre integrated with the Cyber Recovery solution can provide a single pane of dashboard and workflow automation to take coordinated actions based on a predefined set of procedures required to be orchestrated for mock drills and recovery.

CRaaS – Wipro's as a Service model powered by Dell Financial Services help clients reduce Capex expenditures and avail Cyber Recovery as a service in a flexible consumption model

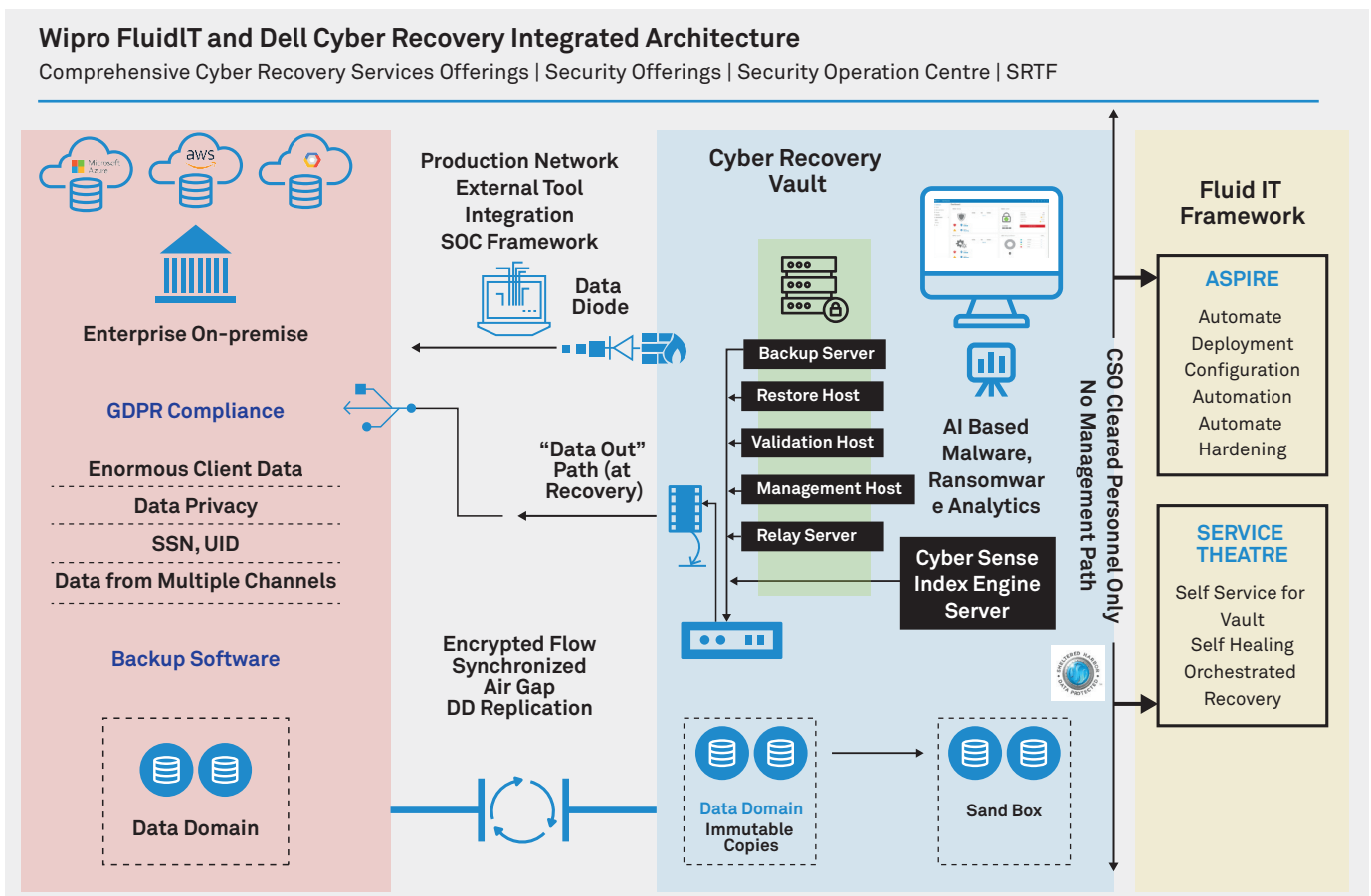


Figure 1: Cyber Recovery Solution Architecture

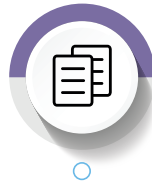
Wipro' Cyber Recovery Services

Pre-Engagement Service Offerings for Wipro CIS



Cyber Recovery Workshop

Gain insights from practical experience in developing your Cyber Recovery program



Cyber Recovery Advisory

Strategic Assessment
Definition of Target State Business Benefits



Pilot Cyber Recovery Services

Prototype of Recovery Services, Target Architecture, Actionable Roadmap

Services Offerings for Wipro CIS



Vault Design and Hardening

Review Security Zone Architecture and integrate best practices for Cyber Recovery Solution and hardening of vault components



Cyber Vault Automation

Automate Cyber Recovery Vault Infrastructure and Deploy air-gap copy and data immutability scripts



Recovery Testing

Develop recovery test plan and conduct knowledge transfer of vault operations, security analytics and restore processes



Project Kick-off and Overview

Review output of Advisory service and identify purpose and function of the Cyber Recovery Vault

Security Response Taskforce

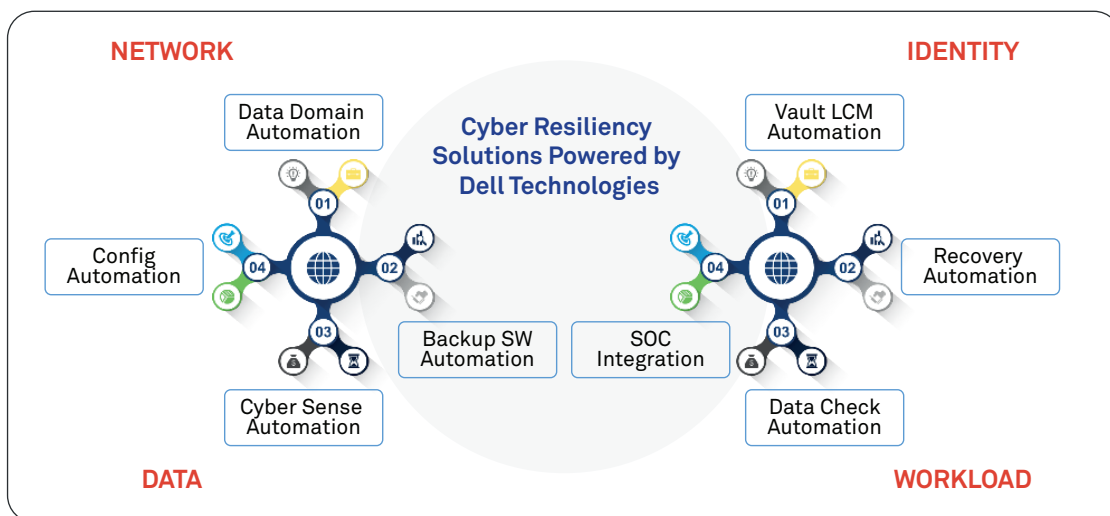


Figure 2: Wipro Network and Security Services – Augmenting Cyber Vault Solutions on Zero Trust Principles

- Robust REST API framework enables analytics with AI/ML for malware (including ransomware)

NETWORK – Zero trust in network security starts with micro-segmentation and the ability to create a defense layer beyond the moat and castle model. The services stack is flexible to provide complete network visibility with enhanced controls and encryption enabled in order to create a true air gap network between entities, thereby preventing any chance of attackers moving laterally across the network

DATA – The security protection protocol of data should ideally be at the same level irrespective where it traverses or resides. Wipro can provide granular data security at all layers comprising controls like data encryption and keys stored on a hardware security module complying with FIPS 140-2 level 3

IDENTITY – People, services, and devices are all constituents of identity. The models ensure that these constituents access resources with the right authentication and are granted access based on the overall policies enforced for any privilege level access violations

WORKLOAD – Once identity is granted, the access to the environment is primal that the security defense at the end points needs to have application centric whitelisting and effective visibility of east of traffic apart from any malware, threats in order to enforced a hardened environment. The model can also take care of risk related to unpatched environment with virtual patching. Wipro can provide comprehensive real time visibility on endpoint host security with deployment of End Point Detection & Response (EDR) with advanced threat intelligence.

Wipro's Fluid IT

The Wipro FluidIT model is based on a programmable software-defined infrastructure framework. It combines Wipro App Anywhere, Wipro Aspire and Wipro Service Theatre modules tightly integrated with various infrastructure components from different OEMs to deliver agile, flexible, and scalable cloud native architecture. These elements form the foundation of an end-to-end, software-defined data center and hybrid cloud. FluidIT weaves infrastructure and applications into a single platform with a comprehensive automation of day 0 to day 2 tasks, all the way up to cloud automation and orchestration.

Deployment automation

Cyber vault deployment automation covering

Data Domain

Backup Software

Configuration automation

Cyber vault elements automation

Service Automation

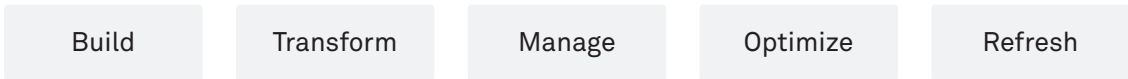
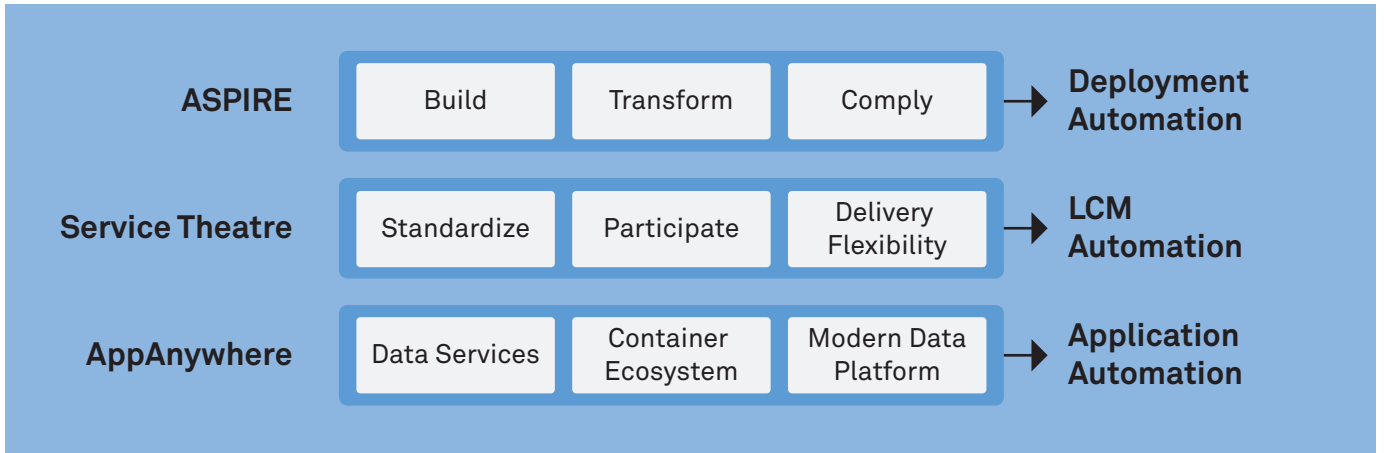
Lifecycle management automation

Recovery automation

Workload data consistency check automation

Out-of-box integration and automation

- Modern UI / UX experience in managing the cyber vault



<p>Speed is the key</p> <p>Match Demand and supply with Build transform Just in Time</p>	<p>Deliver Super efficiency</p> <p>Programmable hardware build with massive scale</p>	<p>Deliver Experience</p> <p>Participate easily with standardized and callable services</p>	<p>Location Agnostic (even databases)</p> <p>Develop and release anywhere driving app consistency</p>
---	--	--	--

● Boost enterprise confidence for a resilient business operation



Full Content Analytics

CyberSense delivers full content-based analytics. This capability sets CyberSense apart from other solutions that take a high-level view of the data and use analytics that look for obvious signs of corruption based on metadata. Metadata-level corruption is not difficult to detect; for instance, changing a file extension to encrypted or radically changing the file size. These types of attacks do not represent the sophisticated attacks that cyber criminals are using today.

CyberSense goes beyond metadata-only solutions because it is based on full-content analytics that provide up to 99.5% confidence in detecting data corruption. It audits files and databases for attacks that include content-only based corruption of the file structure or partial encryption inside a document or page of a database. These attacks cannot be found using analytics that do not scan inside the file to compare how it is changing over time. Without full content-based analytics the number of false negatives will be significant, providing a false sense of confidence in your data integrity and security.

Power Protect Data Domain

Source (production) Data Domain system — The source Data Domain system contains the production data to be protected by the Cyber Recovery solution.

Destination (vault) Data Domain system — The Data Domain system in the CR Vault is the replication target for the source Data Domain system.

- PowerProtect DD meets stringent SLAs with up to 38% faster backups and up to 45% faster restores.
- Higher IOPS with 50% faster instant access /restore with up to 60k IOPS and up to 64 concurrent virtual machines.
- To deliver faster networking compatibility, the new appliances also support 25GbE and 100GbE. PowerProtect DD9900 can support 50% more usable capacity in a single rack, up to 1.5PB of useable capacity and 97.5PB of logical capacity.
- Hardware assisted compression delivers up to 30% more logical capacity per TB across all three new appliances and the rack space is reduced by as much as 39% with new 8TB drives.
- PowerProtect DD also offers grow-in-place expansion through half shelf licensing support.
- PowerProtect DD appliances support the latest update to Dell Technologies EMC Cyber Recovery Solutions with recovery of backups from Cyber Recovery Vault.

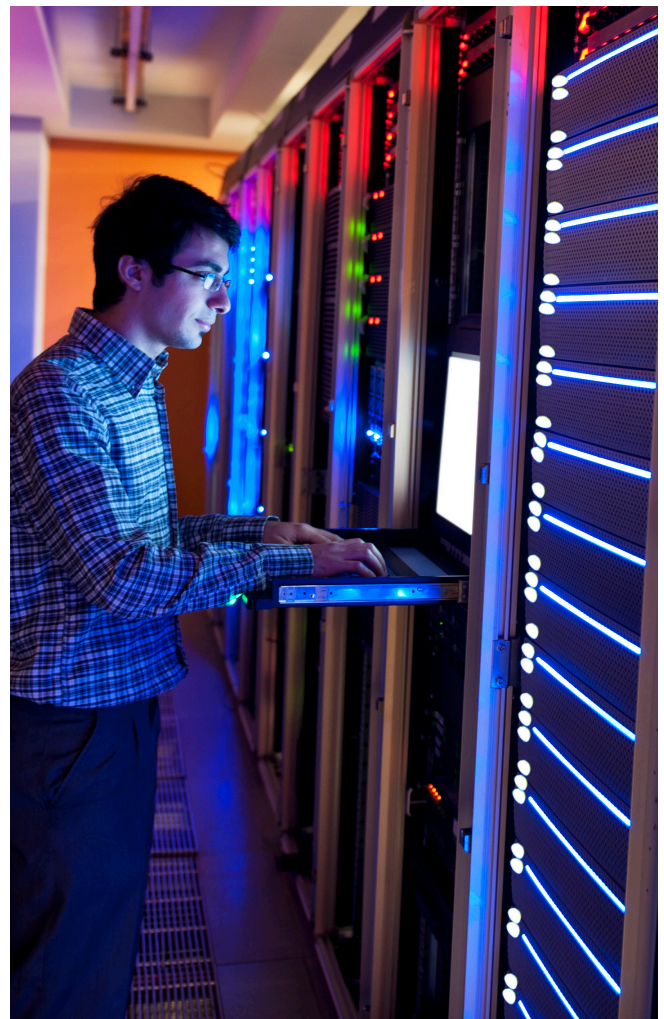
MTree replication—MTree replication is a Data Domain feature that copies unique data from the source Data Domain MTree to the Data Domain MTree in the CR Vault.

Retention Lock (governance or compliance) software—Data Domain Retention Lock software provides data immutability for a specified time. Retention Lock functionality is enabled on a per-MTree basis, and the retention time is set on a per-file basis.

Data immutability — Dell Technologies Cyber Recovery solutions provide both hardware level and software level data immutability as an additional layer of protecting critical data assets. In most of the solutions, you will find only the software feature which also can be compromised if someone gets the administrator credentials.

Cyber Recovery management host—

The management host is where the Cyber Recovery software is installed. This server is installed in the vault environment.



Recovery host—The recovery host is a vault-environment component to which the backup application and data are recovered. Typically, the vault environment includes multiple recovery hosts.

Analytics/indexing host—The analytics/indexing host is an optional but strongly recommended component in the vault environment.

Analytics/indexing host with the data-analysis software that is installed provides direct integration between the Cyber Recovery software and the CyberSense software. Additional analytics/indexing hosts with different tools can also be used as needed.

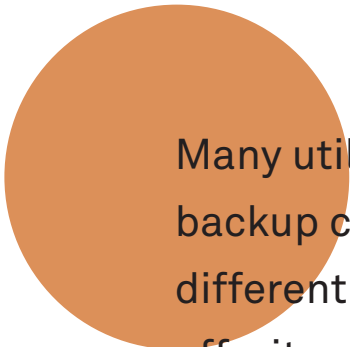
Supported Data Types

CyberSense generates analytics from a comprehensive range of data types. This includes core infrastructure such as DNS, LDAP, Active Directory; unstructured files such as documents, contracts and agreements and intellectual property and databases such as Oracle, DB2, SQL, Epic Cache, and others.

Recovery, Remediation and Automation –

PowerProtect Cyber Recovery provides automated restore and recovery procedures to bring business critical systems back online quickly and with confidence. As part of PowerProtect Data Manager and for customers running Dell Technologies EMC Networker Cyber Recovery, it enables automated recovery from the vault. Dell Technologies EMC and its ecosystem partners provide a comprehensive methodology for protecting data, as well as performing damage assessments and forensics to either recover your systems or remediate and remove the offending malware. Cyber Recovery’s

automated workflow includes the ability to create sandbox copies that you can use for security analytics. Analytics can automatically be performed on a scheduled basis using integration provided within the Cyber Recovery vault management UI or through native REST APIs. Cyber Recovery applies over 40 heuristics to determine indicators of compromise and alert the user. The rapidly changing threat landscape (over 95% CAGR in ransomware variants) demands an adaptive analytics framework; so Cyber Recovery stays ahead of the bad actor by enabling tools incorporating artificial intelligence (AI) and machine learning (ML) analytics methods to the Cyber Recovery vault.



Many utilize a “3-2-1” rule for backups: Three (3) backup copies minimum, preferably in two (2) different formats, with one (1) of those copies stored off-site or air-gapped from the network powered by a modern and proven CyberSense software

Wipro's FluidIT

Wipro's FluidIT model is based on a programmable software-defined infrastructure framework. It combines Wipro App Anywhere, Wipro Aspire and Wipro Service Theatre modules tightly integrated with various infrastructure components from different OEM to deliver agile, flexible and scalable cloud native architecture. These elements form the foundation of an end-to-end, software-defined data center and hybrid cloud. FluidIT weaves infrastructure and applications into a single platform with a comprehensive automation of day 0 to day 2 tasks, all the way up to cloud automation and orchestration.

- Comprehensive automation from day 0 through day 2 tasks – Bring more efficiency and agility in managing cyber vault platform
- Reduces overall build and deployment time – Leads to faster time to market
- Single pane of management

- Significantly reduces management operational cost
- Greatly reduces skills requirement
- Automation from bare metal build to multi cloud deployments
- Reduces cost of delivery / cost of managed services
- Comprehensive cloud automation and orchestration platform

Wipro's FluidIT
Be smart, manage applications from anywhere

Wipro's FluidIT framework

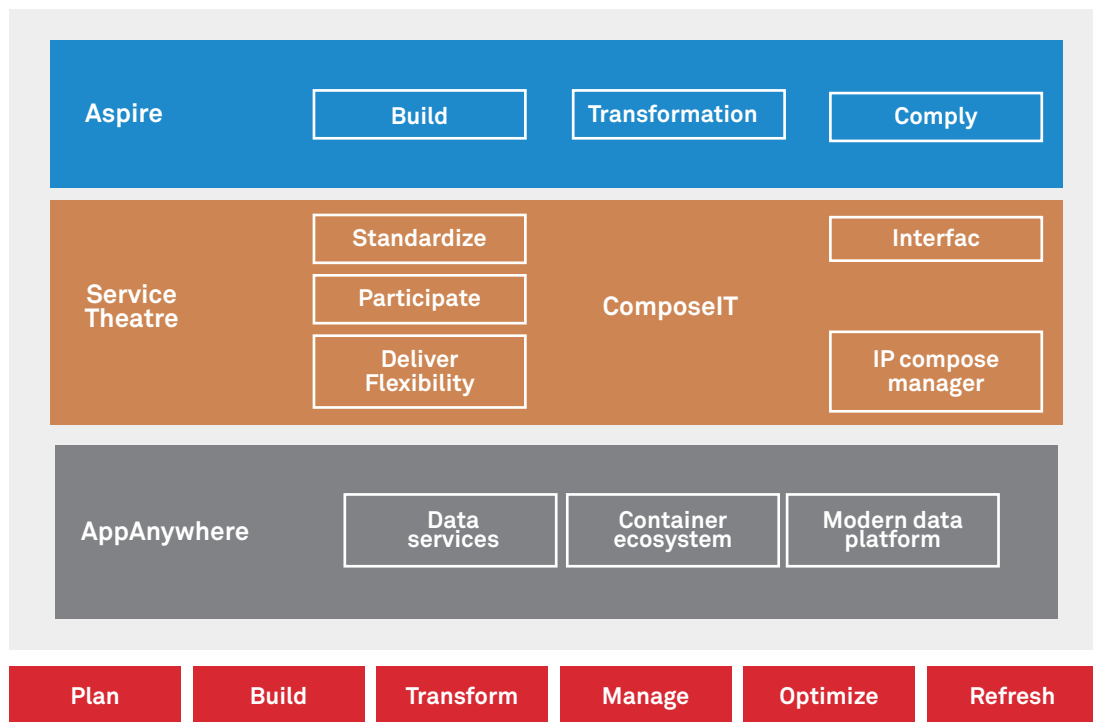


Figure 2: Wipro's FluidIT framework overview



FluidIT framework has 3 high level components

1. ASPIRE 2. Service Theatre 3.AppAnywhere

ASPIRE

ASPIRE is a framework that leverages the programmability of software defined components and automates build integrations. Dell Technologies Cyber recovery solutions components are integrated with Wipro's FluidIT to bring more comprehensive automation across day 0 to day 2 activities.

An automated build process will help in significantly reducing the manual intervention required and reduce the time to deployment to a greater extent.

- Reducing manually intensive deployment procedures
- Hardening OE, catalogue-based deployments
- Comply to client IT governance
- Automated pre-check procedures for patching (Includes process, application shutdown, consistent backup)
 - Patching (N-1). Ex: Patching Linux environments
- Automating the deployment of Cyber Recovery solutions
- Automating power-on to maximum deployment process
- Updating CyberSense signatures
- Improving efficiencies in deployment
- Speeding up large transformation projects

Service Theatre

It is equally capable of performing day 2 tasks (Lifecycle Management) such as

- Hardware updates of Cyber Recovery solution components including hardware and software
- Recursive actionable
- Monitoring and notification – Any notification from CyberSense can be integrated into Service Theatre for triggering further actions
- Interface standardization – Use Wipro Service Theatre to get a unified interface to manage your cyber recovery environment along with other infrastructure components
- Bring in more efficiencies by automating and integrating it with other management frameworks like EMS, SOC and NOC
- Integration and automation of recovery procedures based on alerts, notification and rule-based policy engine

Conclusion

Cyber-attacks are a serious concern for business leaders. They represent a risk that just can't be ignored because the consequences of data and systems unavailability are so costly. But protecting business-critical data against cybercrime is not just a business imperative, it is an exercise fraught with complexity. On the technical side, the limitations of traditional backup and recovery approaches created a need for another line of defense, and it is a defense that is now being widely adopted as a component of a complete approach to cyber recovery—an air-gapped topology with advanced protection, recovery and proactive cyber-analysis capabilities



Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,

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