Wipro Cyber Resiliency Solutions Powered by Dell Technologies

- Solution Brief

CONTENTS

Introduction

Data is the currency of the internet economy and a critical asset that must be protected, kept confidential and made available at a moment's notice. Today's global marketplace relies on the constant flow of data interconnected networks, and digital transformation efforts put more sensitive data at risk. This makes your organization's data an attractive and lucrative target for cyber criminals. Cybercrime has been called the greatest transfer of wealth in history, and it is all about the data. Regardless of the industry or size of the organization, cyber-attacks continually expose business and governments to compromised data, lost revenue due to downtime, reputational damage, and costly regulatory fines. The average annual cost of cybercrime per company increased to US$13M in 2018, a surge of 72% in just the last 5 years. Having a cyber recovery strategy has become a mandate for business and government leaders. 79% of global executives rank cyber-attacks as one of their organization's highest risk management priorities, according to a 2019 Marsh & Microsoft study. So, what can you do to protect your organization and its valuable data?

Why Cyber Recovery

Cyber-attacks are designed to destroy, steal or otherwise compromise your valuable data – including your backups. Protecting your critical data and recovering it with assured integrity is key to resuming normal business operations post-attack. Could your business survive? Here are five components of a proven and modern cyber recovery solution:

Data Isolation and Governance - An isolated data center environment that is disconnected from corporate and backup networks and restricted from users other than those with proper clearance

Automated Data Copy and Air Gap - Create unchangeable data copies in a secure digital vault and processes that create an operational air gap between the production / backup environment and the vault

Intelligent Analytics and Tools - Machine learning and full-content indexing with powerful analytics within the safety of the vault. Automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed

Recovery and Remediation - Workflows and tools to perform recovery after an incident using dynamic restore processes and your existing disaster recovery (DR) procedures

Solution Planning and Design- Expert guidance to select critical data sets, applications and other vital assets to determine (Recovery Time Objective (RTOs) and Recovery Point Objective (RPOs) and streamline recovery

Cyber Recovery Compliments Disaster Recovery

We get a lot of questions about how cyber recovery strategies differ from those of disaster recovery (DR) and always recommend having both plans ready.

For a DR event, you generally know what happened, when it happened and what data was lost. The primary goal of DR is to restore normal operations as soon as possible. In a Cyber Recovery event, you might not know what happened, when it started, or what exactly was lost. The goal is still to restore normal operations as soon as possible, but there are several questions that need to be answered before you know where to begin.

Another critical difference is that cyber recovery vault needs to be isolated from the network and remain physically secure. Any system that is connected to the network is potentially vulnerable to a cyber-attack. Creating an 'air-gap' from the primary network is an effective measure in keeping critical data safe. The vault also needs to be physically secured, and access should be restricted from users without proper clearance.

Cyber recovery solutions must be aimed at recovering the data from a secure isolated vault. This helps customers to resume the business as soon as possible and also provides ample time to the enterprise in taking decisions to negotiate a ransomware or avoid paying a ransomware.

Table 1 summarizes the key difference between disaster recovery and cyber recovery.

	DR	CR
Recovery Time	Close to Instant.	Reliable & Fast
Recovery Point	Ideally Continuous	1 day Average
Nature of Disaster	Flood, Power Outrage, Weather	Cyberattack, Targeted
Impact of Disaster.	Regional, typically contained	Global: Spreads quickly
Topology	Connected, multiple targets	Isolated, in addition to DR
Data Volume	Comprehensive, AI Data.	Selective, Includes Foundation SVCs
Recovery.	Stabdard DR (e.g, failback)	Iterative, selective recovery; part of IR

Table 1: Disaster Recovery Versus Cyber Recovery

Managing Cyber Risk as a Business Issue

There are two key reasons. First, regardless of industry, regulators now focus on cyber security. Today, regulators in financial services, healthcare and utilities / energy are drafting new regulations and increasing their emphasis on cyber security during audits and investigations. Stronger control paradigms will become requirements soon. As a relevant example, the New York State Department of Financial Services Cybersecurity Regulation requires a written cyber security policy to be implemented and maintained, and the board or a senior officer must annually certify compliance.

Second, the potential damage from a successful cyber-attack is so significant that the board must be involved with cybersecurity to fulfill its fiduciary responsibilities. In an extreme case, a successful attack could delete or encrypt the data and systems that the organization must access to operate. Across industries, key systems may include finance and accounting – especially for publicly traded companies with quarterly reporting requirements and Sarbanes-Oxley oversight. There's no room for these systems to be unavailable or lost. Additionally, specific industries depend on systems crucial to ongoing operations.

Critical Data Assets industry Wise

Not limited to, below table shows some of the critical data assets which needs to be protected and categorized as critical data

Retail	**Order management, inventory and fulfillment**
Professional Services (Legal, Consulting)	**Document management, time and billing**
Government / Public and dockets	**Tax rolls, licensing informationSector**
Healthcare	**Electronic medical records, clinical systems**
Utilities	**Smart meter data, interfaces to industrial systems**
Financial Services	**Customer accounts and positions, trading systems and treasury**

Table 2: Industry Wise Critical Data Assets

Dell Technologies is the first technology solution provider to join the Sheltered Harbor Alliance Partner Program.

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

9/10 Organizations using, planning for, testing, or interested in using isolated data recovery solutions

-ESG Dell Technologies Isolated recovery customer research 2019

The solution: Cyber Recovery

Wipro's Cyber Recovery solution powered by Dell Technologies and Wipro's Cyber Recovery services help enable enterprises to battle a joint war against cyber-attacks and protect critical data assets. The solution is an outcome of strong integration of multiple components providing the much-needed cyber recovery resilience, automation and integration with security operation center, unified dashboard, forensic tools, and machine learning techniques. Wipro's FluidIT Service Theatre and Dell Technologies PowerProtect together bring the best-in-class solution in protecting critical data assets.

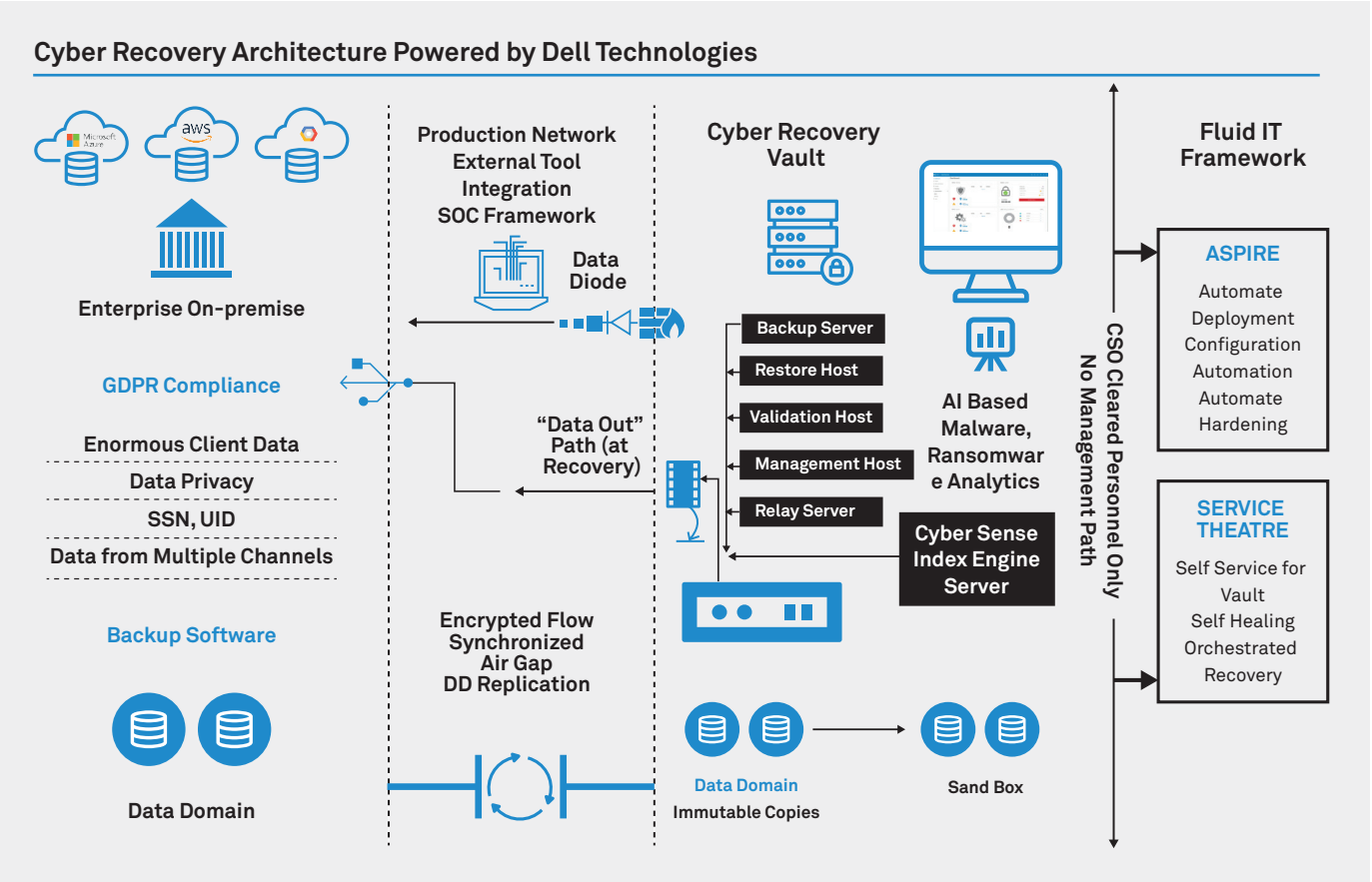


Figure 1: Solution Architecture

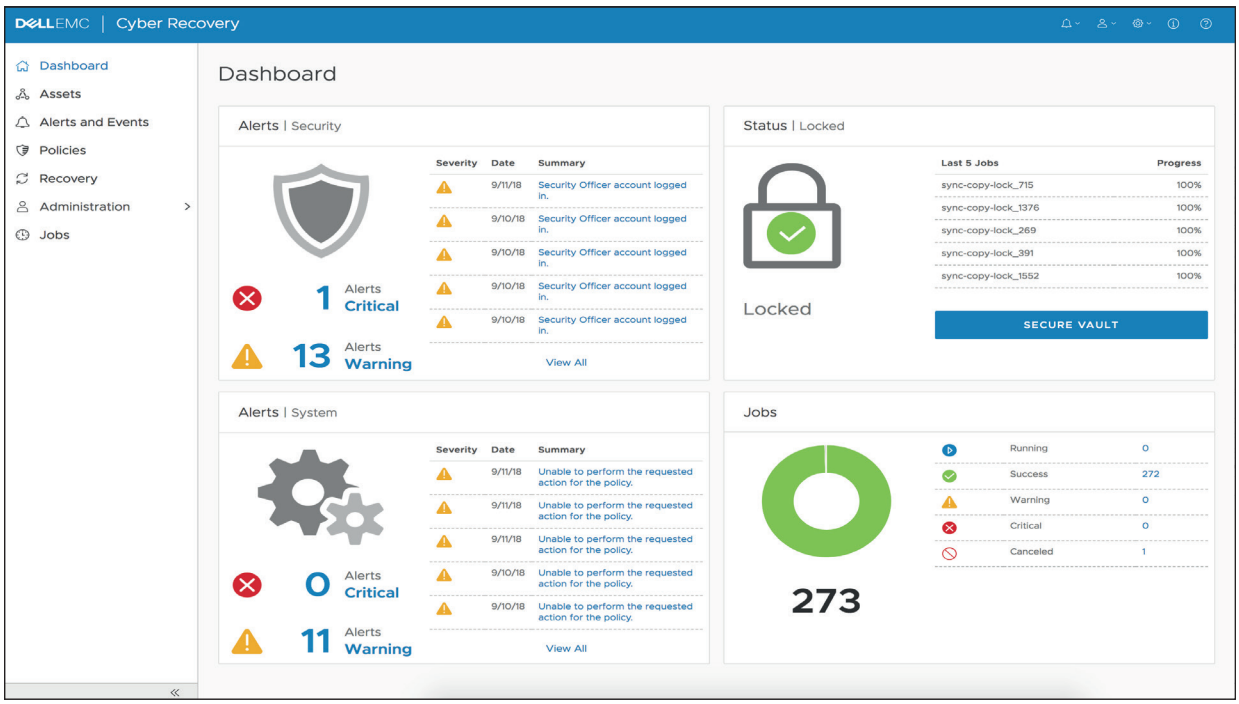
As shown in Figure 1, the base-level Cyber Recovery (CR) solution architecture consists of a pair of data domain systems and the Cyber Recovery management host. In this base-level configuration, the Cyber Recovery software, which runs on the management host, enables and disables the replication Ethernet interface on the data domain system in the CR Vault to control the flow of data from the production environment to the vault environment. Let's look at the functionality of the key components comprising the overall solution.

Data Diode

Using a data diode from OWL Cyber Defense Solutions for secure one-way communication from within the vault environment to the production environment for UDP protocols such as SMTP and SNMP alerts.

Cyber Recovery vault

The PowerProtect Cyber Recovery vault offers multiple layers of protection to provide resilience against cyber-attacks even from an insider threat. It moves critical data away from the attack surface, physically isolating it within a protected part of the data center and requires separate security credentials and multifactor authentication for access. Additional safeguards include an automated operational air gap to provide network isolation and eliminate



CyberSense

PowerProtect Cyber Recovery is the first solution to fully integrate CyberSense which adds an intelligent layer of protection to help find data corruption when an attack penetrates the data center. This innovative approach provides full content indexing and uses machine learning (ML) to analyze over 100 content-based statistics and detect signs of corruption due to ransomware. Analyzing data happens at both metadata and file level and thus CyberSense finds corruption with up to 99.5% confidence, helping you identify threats and diagnose attack vectors while protecting your business-critical content – all within the security of the vault.

CyberSense delivers a unique approach, auditing data content to determine if it has been compromised. Key advantages include:

- Direct scanning of all common backup software images, including Networker and Avamar
- More than 100 statistics generated to look inside the data for unusual behavior
- Machine learning to generate a 'Yes/No' indicator that an attack has occurred
- Forensic tools to find corrupt files and diagnose the attack vector
- Ability to quickly find and restore last good file to minimize business interruption

Automated Data Integrity Audits

CyberSense adds a layer of protection that examines the inside of files and databases to understand how they change over time. CyberSense monitors the integrity of the data and sends alerts when changes occur that are indicative of a cyberattack. This added layer of security is designed to compensate for when attacks circumvent existing security defenses.

CyberSense with Cyber Recovery Workflow

CyberSense is fully integrated with Dell Technologies EMC Cyber Recovery and monitors files and databases to determine if an attack has occurred based on data corruption. Once data is replicated to the Cyber Recovery vault and the retention lock is applied, CyberSense scans the backup data, creating point-in-time observations of files and databases. This scan occurs directly on the data within the backup image without the need for the original backup software. Analytics are generated, including file type mismatch, corruption, known ransomware extensions, deletions, entropy, similarity, and more.

The analytics are then used by machine learning algorithms to make a deterministic decision on data corruption that is indicative of a cyberattack. The machine learning algorithms have been trained by all the latest trojans and ransomware and can be updated as new attack vectors are discovered. Observations of the data allow CyberSense to track how contents of files change over time. If an attack occurs, a critical alert is displayed in the Cyber Recovery dashboard and CyberSense post-attack forensic reports are available to quickly diagnose and recover from the ransomware attack.

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.

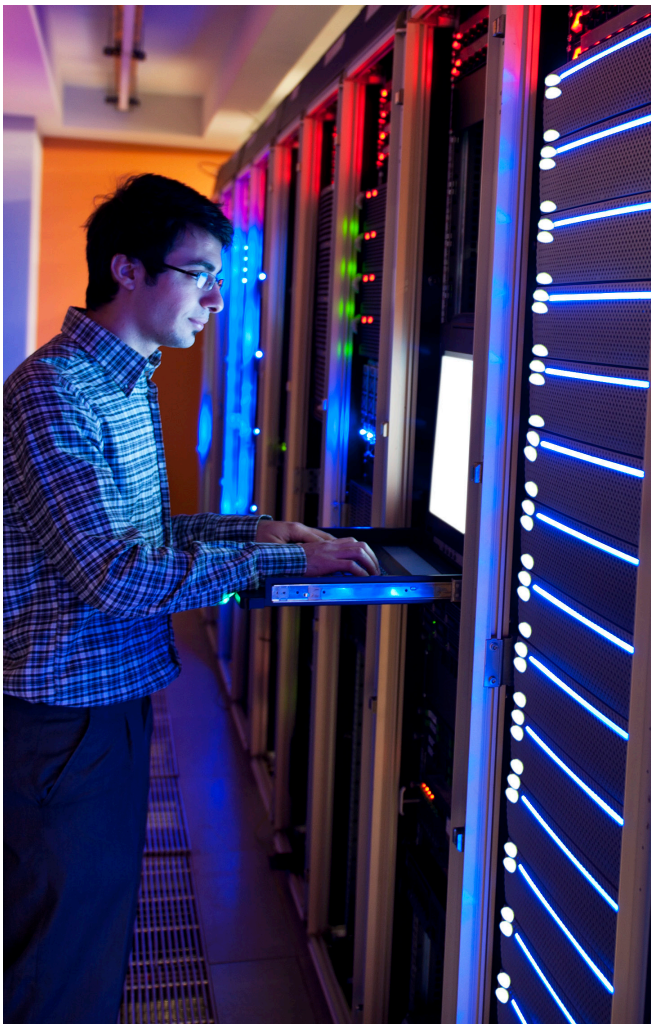
- PowerProtect DD meets stringent SLAs with up to 38% faster backups and up to 45% faster restores.
- Higher IOPS with 50% faster instant access /restore with up to 60k IOPS and up to 64 concurrent virtual machines.
- To deliver faster networking compatibility, the new appliances also support 25GbE and 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

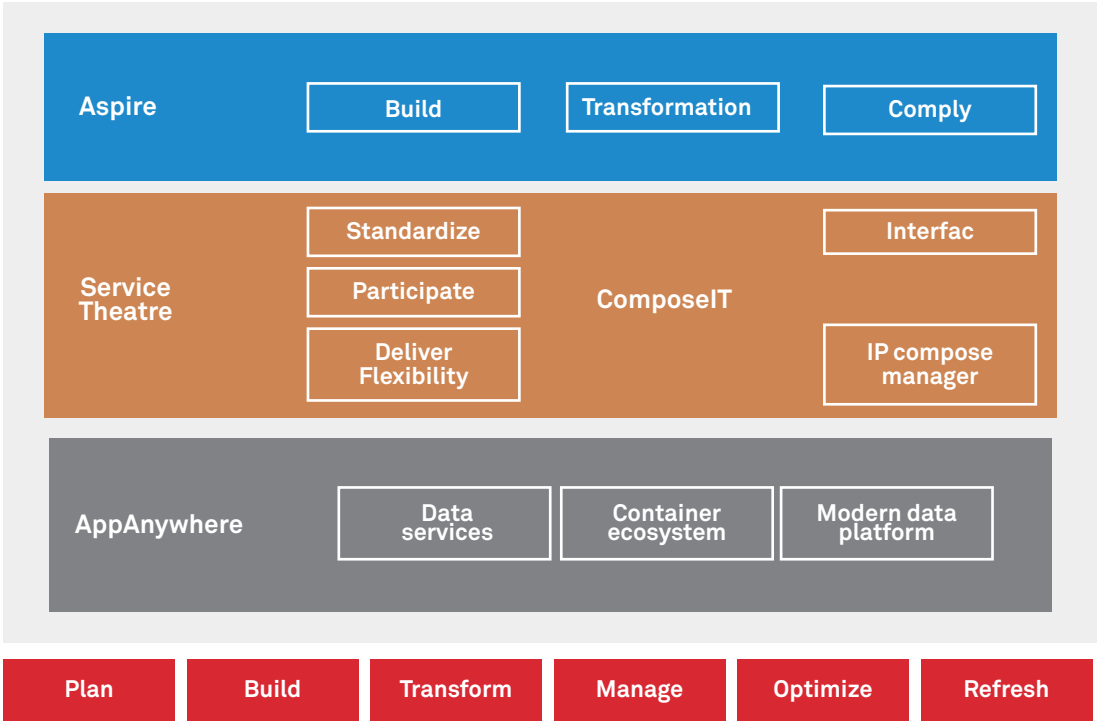


Figure 2: Wipro's FluidIT framework overview

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

AppAnywhere

AppAnywhere delivers the agility, cost savings, and flexibility leveraging on cloud native architecture principle that allows enterprises to build, deploy and operate cloud native applications in the multi-cloud or hybrid-cloud environments of their choice, free from lock-in into underlying systems. Its offered by Wipro on a managed services model comprising of tightly integrated technologies that together deliver end-to-end automation of IT lifecycle to enterprises.

Conclusion

Assurance and confidence to recover business critical data and systems post a Cyber related incidence poses a serious concern for business leaders. The velocity and impact of cyberattacks continues to rise with newer techniques and tactics are exploited to expands the horizon of threat surface. Amongst the prevailing cyber threat,ransomware continues to be integral part of attacker's strategy.

This represent a risk that just can't be ignored since the consequences of such cyber breaches are far more devasting which goes beyond data and systems corruption apart from cost of recovering.

Hence protecting business-critical data against impeding cyber threat is not just a business imperative, it is an exercise fraught with FUD – Fear, Uncertainty and Doubt to resume normalcy and business as usual state.

On the technical side, the limitations of traditional backup and recovery are potent elements to get compromised once the cyber adversary moves towards final execution and eventually compromising system through command and control as per the cyber kill chain process. Cyber Resiliency stipulate a need for a line defense Cyber Recovery Vault which is now being widely adopted for a holistic approach which encompasses —an air-gapped topology with advanced protection, recovery, and a proactive cyber-analysis capabilities to detect behavioral change linked to anomalies for data protected.

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**

IND/TBS/MAY-DEC 2020