The command center of the future

wipro

When an IT engineer pulled a wrong plug in the data center of a leading airline, little did he know that it would leave 75,000 passengers stranded, hundreds of flights cancelled and the airline would incur a loss worth more than $100 Million. How did it all start? who asked the engineer to pull the plug? Did he do an impact analysis? Why did the command center take more than a day to recognize the problem, take action and restore service? Could they have done any better? Were they prepared to deal with a human error like this?

The incident relates to a common fact that many organizations still run multiple command centers in silos with minimal information exchange. Some examples of silo command centers are network command center, applications command center, facilities command center, business command center, cloud command center, and datacenter command center. Each command center brings with it its own service owners, its own tools/processes, its own technologies and seldom can these interact and exchange data with each other.

This leads to a potential situation where a network command center will never know about a power outage in a data center, which can potentially affect the availability of servers, applications, and at the end of it all, the business. In the incident referred above, while the airline could not have prevented the human error, it would have taken much lesser time to find the root cause of the incident and fix the problem if the multiple command centers were integrated.

How can we address such problems?

Today data is flowing across the ecosystem at the speed of light. Sensors, mobiles, smart watches, smart buildings, air conditioners, servers and applications are all sending user data, consumer data, and device data. Collecting this huge amount of data, available across multiple sources and within command centers, at one place, analyzing it, processing the meaningful data and generating insights for the command center is the biggest challenge.

Companies of the future will be able to collect data such as consumer data, business data, IT data, facilities data, and marketing data; interpret the data, find anomalies and patterns, perform data correlation, and present it back to a single command center (which can have specialized groups such as network command center). This will improve the ability to predict outages, disruptions and take corrective decisions quickly and intelligently.

Building the next-gen command center

To enable a more intelligent next-gen global command center, organizations need to rethink the strategy around how they conceptualize command centers. Here are some of the building blocks that will frame the command center of the future (see Figure 1):

Data aggregation layer – This layer will comprise tools and technologies that will collect data from multiple sources like IoT devices, applications logs, security threats, cloud alerts, facilities alerts.

Event correlation layer – This layer will have the capability to process the data, filter the anomalies, remediate some of the common problems, contextualize the remaining alerts to a business application and assign it to the best available teams who can solve the problem quickly through cognitive capability.

Prediction layer – Artificial Intelligence will determine anomalies in the behavior of IT estate and pattern of faults to predict future outages and performance issues in this layer.

Service management layer – This layer will base on IT4IT reference architecture. Key aspects like Self Service, Service Request Management, Incident Management, Change Management, Configuration Management and Knowledge Management will continue to drive command centers.

A command center will have a 360º view of applications and all underlying components that potentially impact service availability.

Automation layer – This layer will take quick actions on the intelligence provided by the event correlation layer. Whether it is to execute a remediation script, to generate an outage alert to the Major Incident Management team to initiate quickly a fallback strategy, the automation layer will take actions that a normal human would do.

Cost management layer – This layer will manage the cost impact of changes in an enterprise. For example, how much does it cost to add or remove a server on cloud? What cost impact will it have on the business? What budgets are required to manage these changes?

Audit and compliance layer – This layer will ensure that the audit of the enterprise meets the objectives of the business. For example: audit rules will be setup to ensure IT/Facilities make no changes during critical business hours.

Intent based policy and configurations – Encouraged by 'intent based networking', companies will define intents within the command center instead of focusing on silo availability of infrastructure or applications. For example, a company will define an intent as, "ensure the transaction response on the web application does not go above two milliseconds." For this intent, policies on all impacted underlying components like applications, servers, databases, networks would be defined. Also, search rules to learn about the user experience on the transaction page and interactions on social media would be defined. These policies will be irrespective of which tool is used to monitor and manage the enterprise.

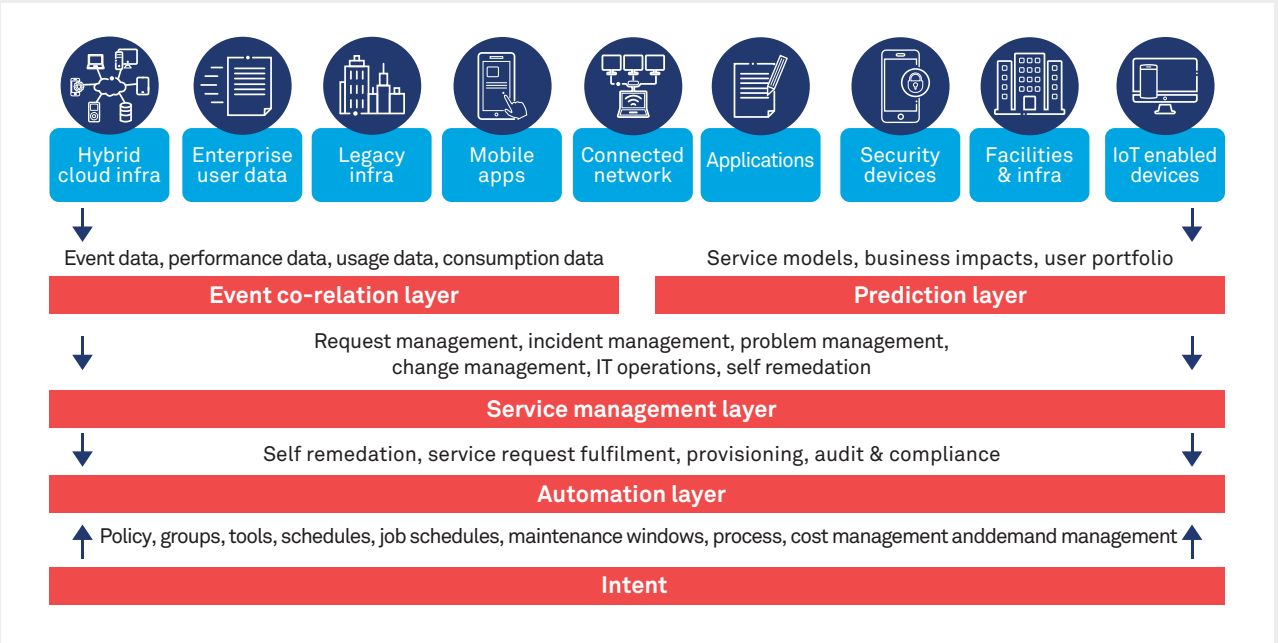

Figure 1: Building blocks of the command center of the future

Through these building blocks, the companies will be able to achieve a command center that provides the following capabilities:

Contextual: Majority of enterprises and business applications will be re-engineered to be cloud-ready and micro-services-ready, and built for containers. These applications will be consumed through multiple channels by users, machines, and devices. A command center will have a 360º view of applications and all underlying components that potentially impact service availability. Hence, underlying tools (including application performance management tools, infrastructure management tools, security management tools, user experience management tools, social media watchdog tools, IoT management tools) and technology platforms will be service context aware and scalable to handle data at volume. Command centers will get the power to perform deep dive diagnostics of the alerts generated by business applications across multiple geographies when these applications are consumed by different profiles of users. These alerts will be contextualized with other alerts coming in from sources such as malware alert tools and will be managed in the same platform.

Complete: The command center tools and technology platforms will be compatible with all technologies (OEM, Public Cloud, PaaS, Open Source, Containers, Micro-services, Java apps, Network, IoT data, Software Defined Infra) and will be able to correlate the pattern of data, structure of events, derive consumable data, and define data structures that can be passed on to capacity, prediction and automation layers.

Secure: The command center tools and technology platform will be secure, robust, and highly available, will protect data, avoid duplication, protect privacy laws, and be foolproof against attacks.

Predictive: One of the major responsibilities of a command center is not only to react to major outages, but also to be predictive and prevent outages. Hence predictive solutions (doing trend analysis of events, configuration change analytics, anomaly detection, service consumption pattern analysis, seasonal analytics, and behavior analytics) will empower the command center to predict issues much faster and take corrective actions.

Automated: Automation is the most powerful, at the same time, most complex part of a network command center. From performing routine health checks and housekeeping tasks (disk space analysis, network bandwidth analysis) to more complex tasks (like cognitive computing, machine learning to teach system about similar outages and potential solutions), automation will be carefully designed and executed. Legacy orchestration solutions will continue to exist, but will soon give way to Robotic Process Automation solutions.

Enterprise command center

While technologies become complex, IT becomes bimodal, and user behavior drives IT consumption, global command center will evolve to be an enterprise command center where every action or alert will be considered as a threat to the enterprise and predictive tools will be put to use to drive IT as IT operations analytics than a reactive task force.

About the author

Tarush Gupta
Practice Director,
Global Infrastructure Services, Wipro Ltd.

Tarush has led the Business Service Management practice at Wipro for the past two years, and has played a key role in developing next generation tools and automation offerings through Artificial Intelligence (AI), Machine Learning and Cognitive platforms. He has led large automation transformation programs from concept through implementation. His current focus areas include intent aware tooling, AI Ops and Enterprise Service Management.
You can reach Tarush at
tarush.gupta@wipro.com

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 160,000 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/B&T/MAR-AUG2018