

Galaxy and Commvault

organized highly anticipated roadshow with insightful conversations and thought-provoking debates, the panel shed light on strategies, best practices, and future trends in data management.



Anoop Pai Dhungat
Chairman & Managing Director

Dear Readers,

At the outset, I would like to wish all of you a very Happy Diwali and wonderful year ahead. The reality of climate change and pollution has hit home hard this year. Mumbai, which was relatively unaffected thanks to its proximity to the sea has been badly affected. As usual, there are knee jerk reactions that will offer optical relief in the short term and absolutely nothing in the long term. Mumbai & Delhi desperately need a master plan that requires strict implementation of pollution norms for construction, transportation vehicles and garbage disposal. Let's hope to see some improvements this year that will give us some respite in the future.

Last month, we saw the biggest and most brazen act of terrorism since the Mumbai attacks. What astounds me is that with all the modern technology and artificial intelligence tools available, such an attack could not be forewarned or prevented. It is also extremely sad that such technology could not or was not used to target just the terrorists and instead caused a huge humanitarian crisis. I wish that instead of spending time on deepfakes and other counterproductive things, AI should be used to analyse all available data like satellite imagery, radio chatter, social media feeds, news from various sources and then predict and prevent attacks by identifying the acts and perpetrators beforehand. And that too, without impacting the privacy of most of the people!

Enjoy the festivities.

Happy Reading



Future is Now

How AI Is Changing The Future Of Work

We've been hearing for years the warning that a robot might take over our job. More recently, a report by Goldman Sachs suggested that artificial intelligence (AI) could replace a staggering 300 million full time jobs. Yet for many people, work has seemed to mostly chug along as normal.

Is it all just hype? Or are we finally hitting the inflection point with recent advances in AI? And will AI replace us, or actually make us better and faster at what we do?

► **Expect a role reversal: we'll soon be the ones assisting machines, not vice versa** : We will see a paradigm shift from machines assisting humans to humans assisting machines in the next decade.

► **AI's impact will be as big as the Industrial Revolution, empowering one to do the work of many** : AI is a force multiplier for human intelligence and productivity. Like the Industrial Revolution brought with machines and factories, AI is a means of production that will empower one to do the work of many.

► **AI will reach across industries** : The potential for AI to automate, personalize and fine-tune thousands of processes in industries as widespread as healthcare, education, infrastructure and professional services.

► **White collar job functions, from coding to financial services to legal, will become vastly more efficient** : In areas like financial services and legal, the days of manual research are numbered as the collaboration between professionals and AI-native applications will streamline (and in some cases eliminate) job functions to create previously unimaginable efficiencies.

► **AI is already reducing the number of junior and mid-level software developers needed to ship new products** : One immediate impact of large language models (LLMs) is that they are significantly reducing the number of software developers needed to build and ship new digital products.

► **As GenAI disrupts traditional roles, professionals will lean on AI-powered peer-to-peer channels to learn, up-skill and navigate new career paths** : Generative AI will accelerate personalized and applied

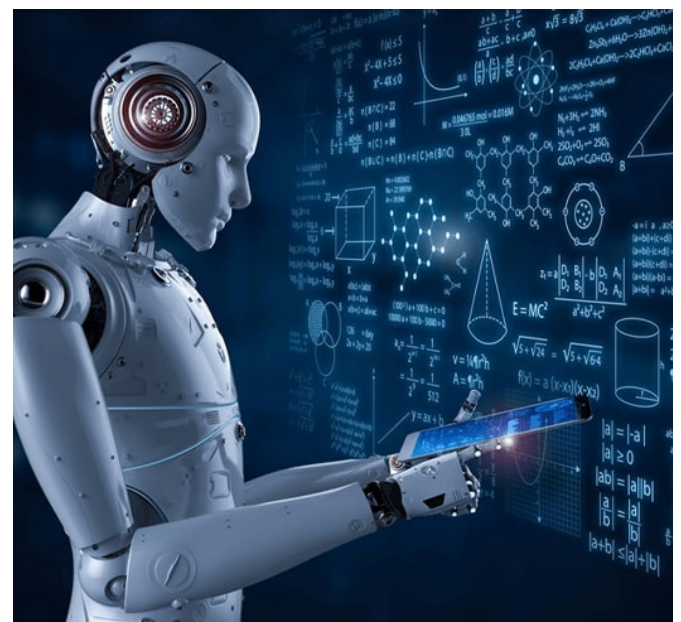
learning both inside and outside of the workplace.

► **AI transforms the way organizations make critical decisions** : AI powers simulations that feed insights and proposals into commercial decisions like exploring pricing schemes, operational ones like optimizing routing and logistics and even those in more complex domains like finding design and engineering solutions to a detailed brief.

► **AI is making it harder than ever to identify substance amidst all the noise** : Great innovation can be obtained by these disruptor trends (AI machine learning, automation, etc.).

► **Large language models are not just hype** : It is apparent to everyone that large language models are a once-in-a-generation technology. Any startup or VC that believes they are just hype, and therefore can be ignored, has their head in the sand.

► **AI will impact our day-to-day work, first gradually, and then suddenly** : Jobs don't disappear overnight. First there's a slow culling, with intermediate steps like offshoring. Eventually technology reaches enough maturity, and business processes change sufficiently, resulting in a rapid decline.



<https://tinyurl.com/4fs9ft9m>

NoSQL Unleashed: Exploring the World of Non-Relational Data Stores

NoSQL, also referred to as “not only SQL,” “non-SQL,” is an approach to database design that enables the storage and querying of data outside the traditional structures found in relational databases. While it can still store data found within relational database management systems (RDBMS), it just stores it differently compared to an RDBMS. The decision to use a relational database versus a non-relational database is largely contextual, and it varies depending on the use case.

Instead of the typical tabular structure of a relational database, NoSQL databases, house data within one data structure, such as JSON document. Since this non-relational database design does not require a schema, it offers rapid scalability to manage large and typically unstructured data sets.

NoSQL is also type of distributed database, which means that information is copied and stored on various servers, which can be remote or local. This ensures availability and reliability of data. If some of the data goes offline, the rest of the database can continue to run.

Today, companies need to manage large data volumes at high speeds with the ability to scale up quickly to run modern web applications in nearly every industry. In this era of growth within cloud, big data, and mobile and web applications, NoSQL databases provide that speed and scalability, making it a popular choice for their performance and ease of use.

Advantages of NoSQL

Each type of NoSQL database has strengths that make it better for specific use cases. However, they all share the following advantages for developers and create the framework to provide better service customers, including:

► **Cost-effectiveness:** It is expensive to maintain high-end, commercial RDBMS. They require the purchase of licenses, trained database managers, and powerful hardware to scale vertically. NoSQL databases allow you to quickly scale horizontally, better allocating resources to minimize costs.

► **Flexibility:** Horizontal scaling and a flexible data model also mean NoSQL databases can address large volumes of rapidly changing data, making them great for agile

development, quick iterations, and frequent code pushes.

► **Replication:** NoSQL replication functionality copies and stores data across multiple servers. This replication provides data reliability, ensuring access during down time and protecting against data loss if servers go offline.

► **Speed:** NoSQL enables faster, more agile storage and processing for all users, from developers to sales teams to customers. Speed also makes NoSQL databases generally a better fit for modern, complex web applications, e-commerce sites, or mobile applications.

In a nutshell, NoSQL databases provide high performance, availability, and scalability.

NoSQL use cases

The structure and type of NoSQL database you choose will depend on how your organization plans to use it. Here are some specific uses for various types of NoSQL databases.

► **Managing data relationships:** Managing the complex aggregation of data and the relationships between these points is typically handled with a graph-based NoSQL database. This includes recommendation engines, knowledge graphs, fraud detection applications, and social networks, where connections are made between people using various data types.

► **Low-latency performance:** Gaming, home fitness applications, and ad technology all require high throughput for real-time data management. This infrastructure provides the greatest value to the consumer, whether that’s market bidding updates or returning the most relevant ads. Web applications require in-memory NoSQL databases to provide rapid response time and manage spikes in usage without the lag that can come with disk storage.

► **Scaling and large data volumes:** E-commerce requires the ability to manage huge spikes in usage, whether it’s for a one-day sale or the holiday shopping season. Key-value databases are frequently used in e-commerce applications because its simple structure is easily scaled up during times of heavy traffic. This agility is valuable to gaming, adtech, and Internet of Things (IoT) applications.

<https://tinyurl.com/mu7p842p>

Fortinet Secure SD-WAN & Secured SD-Branches

Fortinet's consolidated branch security solutions are designed to provide comprehensive security for multiple branches across a country or even globally. These solutions aim to secure the network infrastructure, endpoints (devices), and provide centralized control and management for all branch locations. Here are key components and features of Fortinet's consolidated branch security solution:

► **Unified Threat Protection:** Fortinet's solution offers a wide range of security tools, including firewalls, intrusion prevention systems (IPS), antivirus, web filtering, email security, and more. These tools work together to protect the network from various threats, such as malware, phishing, and advanced threats.

► **Centralized Management:** The solution provides a centralized management platform that allows administrators to define and enforce security policies consistently across all branch locations. This simplifies configuration and policy management for distributed networks.

► **SD-WAN Integration:** Many of Fortinet's branch security solutions include SD-WAN capabilities, allowing for efficient and secure branch-to-branch communication, as well as optimized connectivity to cloud resources. This enhances network performance while maintaining security.

► **Endpoint Security:** Fortinet's solution often includes endpoint security features, such as endpoint protection platforms (EPP) and endpoint detection and response (EDR) capabilities, to secure devices used by branch employees, ensuring that endpoints are protected both within and outside the branch network.

► **Secure Remote Access:** The solution provides secure remote access options for branch employees who need to connect to the network from outside the branch office. This includes VPN and Zero Trust Network Access (ZTNA) solutions to ensure secure and authenticated access.

► **Security Fabric Integration:** Fortinet's branch security solutions are often part of the larger Security Fabric

ecosystem, allowing for seamless integration with other Fortinet security products and services. This integration enhances threat intelligence sharing and incident response capabilities.

► **Scalability:** The solution is designed to scale as your organization grows. It can accommodate additional branch locations and resources while maintaining consistent security policies and protection.

► **Cloud Integration:** Fortinet's solutions are designed to work with cloud services and applications, allowing branches to securely access cloud resources while ensuring data security and compliance.

► **Security Analytics and Reporting:** The solution includes analytics and reporting tools that provide insights into security events, network performance, and compliance status. This data is critical for monitoring and fine-tuning security measures.

► **Compliance and Regulatory Support:** Fortinet's solutions often include features to help organizations meet various compliance and regulatory requirements, which is important for industries with specific security mandates.

Fortinet's consolidated branch security solutions are a valuable option for organizations with multiple branch offices that need consistent, robust, and centralized security across their entire network. These solutions offer a unified approach to network security, endpoint protection, and remote access while providing the scalability and flexibility required to adapt to changing business needs and the evolving threat landscape.

Fortinet Security Fabric

Fortinet's Security Fabric is a comprehensive and integrated security platform designed to provide network security solutions across a wide range of products and services. It offers a holistic approach to security, enabling organizations to effectively protect their network infrastructure, data, and applications. Here are some key components and features of the Fortinet Security Fabric:

► **Unified Management:** The Security Fabric provides a unified management interface that allows administrators to oversee and control various security products and services from a single dashboard. This simplifies the management of security policies and configurations.

► **Multi-Layered Security:** Fortinet's Security Fabric includes a variety of security solutions, such as firewalls, intrusion prevention systems (IPS), antivirus, web filtering, email security, and more. These multiple layers of security help protect against a wide range of threats, including malware, ransomware, and advanced persistent threats (APTs).

► **Scalability:** The platform is designed to scale with the organization's needs, making it suitable for small businesses, enterprises, and service providers. You can add additional Fortinet products as your network grows.

► **Integration:** Fortinet promotes the integration of its products and services, ensuring that they work together seamlessly to provide better threat intelligence, threat detection, and response capabilities. This integration enhances the overall security posture of the network.

► **Security Fabric Ecosystem:** Fortinet collaborates with a wide range of technology partners and offers APIs to allow third-party security products to integrate with the Security Fabric. This ecosystem approach enables organizations to add complementary security solutions and extend their security capabilities.

► **Single Sign-On (SSO):** The Security Fabric supports

single sign-on, allowing users to access various applications and services with a single set of credentials, simplifying user management and enhancing security.

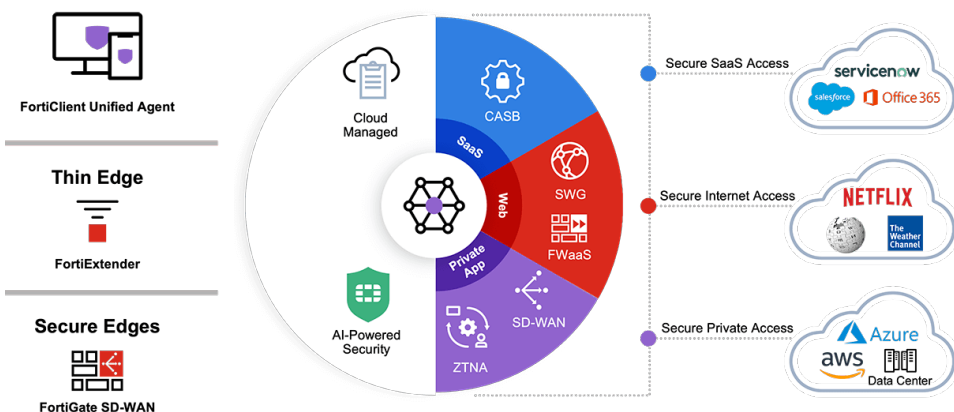
► **Security Analytics:** Fortinet's platform provides advanced analytics and reporting capabilities to help organizations gain insights into their network traffic and security events. This data is crucial for identifying and responding to security threats.

► **Security Automation:** The Security Fabric can automate threat response and remediation actions, reducing the time it takes to react to security incidents and minimizing potential damage.

► **Zero Trust Network Access (ZTNA):** The platform incorporates ZTNA principles to ensure that users and devices only access the resources they are authorized to access, even when connecting remotely.

► **Secure Access Service Edge (SASE):** Fortinet also supports the SASE model, which combines network security and wide-area networking into a unified cloud-based service, allowing organizations to securely connect users and devices to cloud applications and data.

Fortinet's Security Fabric is a powerful and flexible solution for organizations looking to bolster their network security and protect against the evolving threat landscape. It provides a holistic approach to security that integrates various components and services into a unified platform, making it easier to manage and enhance the overall security posture.



Galaxy provides scalability and flexibility required to adapt to changing business needs and the evolving threat landscape with unified approach to network security and endpoint protection. To talk to our experts, email us at marketing@goapl.com



Cisco launches Secure Networking approach in India

Cisco has launched its Secure Networking approach in India, an innovative offer that combines advanced capabilities of networking and cybersecurity. The offer is built on the concept of zero trust to provide businesses with seamless and secure connectivity to tackle the risks of cybersecurity in a hybrid world.

Amid the dynamic and expanding threat landscape, businesses face a core challenge: strengthening their IT infrastructure to remain resilient in a hybrid world. With employees working from different locations, using multiple connections, and accessing information across diverse platforms, resiliency becomes even more critical. Here, the network plays a crucial role as the first line of defense and the sole control point that comprehensively monitors every connection, be it users, devices, or entities.

“One of Cisco's unique differentiators is its unmatched visibility of the network, which allows us to secure everything that's connected. With Cisco Secure Networking, we are bringing together security capabilities including the ability to apply zero trust principles and enforce granular security policies into a single console,” said Vish Iyer, President of Architectures, Asia Pacific, Japan and China at Cisco.

Companies in India are not ready to fully tackle the cybersecurity challenge. According to Cisco's Cybersecurity Readiness Index, which launched earlier this year, only 24% of organizations in India have a 'Mature' level of readiness needed to be resilient against today's modern cybersecurity risks. This readiness gap is telling, not least because 90% of the respondents in India said they expect a cybersecurity incident to disrupt their business in the next 12 to 24 months.

<https://tinyurl.com/mr27bcb3>

IT hardware companies may require global certification

The government may ask laptop, server and other IT hardware importers to provide an international certification attesting that their product is from a trusted source before allowing a licence-free import of it, people in the know of the matter told ET.

This certification, one of the people said, could be from an international organisation. This organisation could periodically verify that the components used in the hardware come from trusted supply chains and do not have any spyware or malware in them, this person said.

The move is aimed at providing a workable solution to countries such as China, the US, South Korea and Taiwan.

They had, at a meeting of the World Trade Organization's Committee on Market Access earlier this week, raised India's decision to put restrictions on the import of these products. They claimed that the decision would have an impact on the trade of these products, cause uncertainty for their users as well as exporters, and was inconsistent with global trade laws.

Sources said some of the hardware could potentially have security related issues and could compromise sensitive and personal data. Clarity on the regulations is crucial before the import management system for IT products kicks in from November and for allaying the concerns of the exporting nations.

The US has said the measure would prompt its firms to think twice about doing business in India, and that it would impact its exports to India. While South Korea raised doubts about the decision's consistency with WTO rules, China and Taiwan asked about the purpose of this policy

<https://tinyurl.com/bdd9zd4y>

All product names, logos, brands, trademarks, and registered trademarks are property of their respective owners.



A-23/24, Ambika Towers, Ground Floor,
Off. Jijamata Road, Nr, Pump House,
Andheri (E), Mumbai - 400 093, India.



91-22-42187777



marketing@goapl.com



www.goapl.com