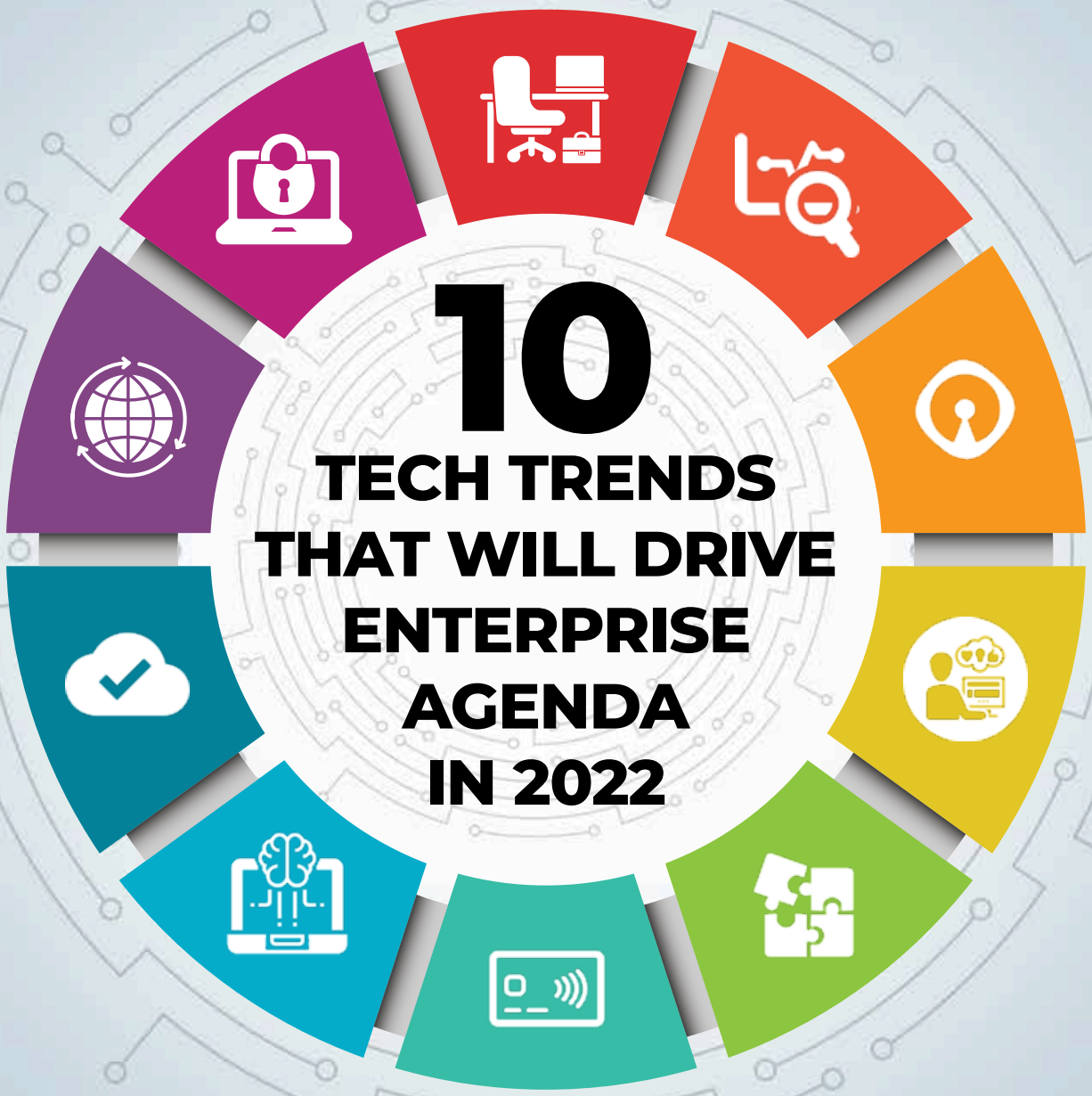
Insight | Pg 14
The Urgency Of Securing Evolving Workplaces

Insight | Pg 26
Addressing WFA IT Pain Points With SD-WAN And ZTNA

ITNEXT
FOR THE NEXT GENERATION OF CIOs



10 TECH TRENDS THAT WILL DRIVE ENTERPRISE AGENDA IN 2022

November 2021 | ₹100 | Volume 12 | Issue 08 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

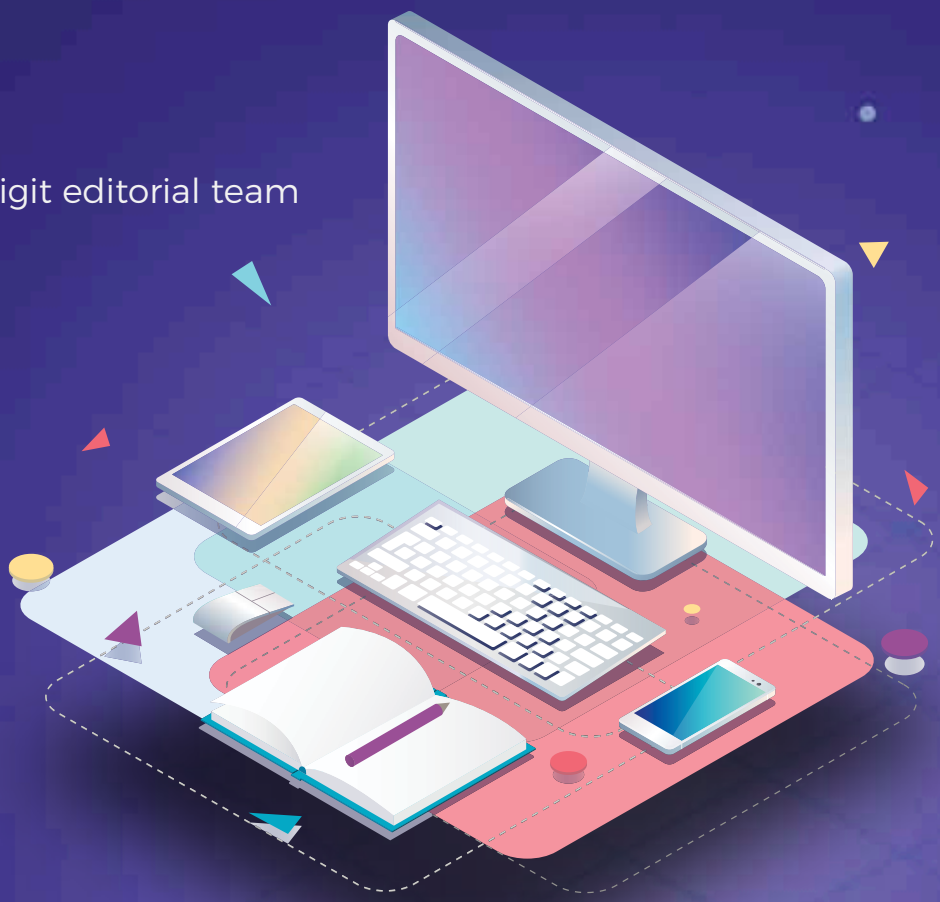
LAUNCHING

digit SQUAD

Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member

- Launch your own tech channel on Digit.in
- Become a Digit Certified tech influencer
- Engage with digit editorial team
- Make money



Apply now by scanning the QR code

www.digit.in/digit-squad/apply.html

Defending the F-word

Some trends are already visible. Some could happen in 2023 or 2024, because of a number of parameters impacting them. It is not that they will be there only between 1st January 2022 and 31st December 2022

Shyamanuja Das

Sometime around 2004-05, I did a forecasting story on then booming Indian BPO industry. The CEO of one BPO company, who claimed (and I would love to believe him) that he always read my stories, called me and asked – if it was what I thought would happen or is it what I thought should happen. While I was trying to evade, he provided me the answer.

"Maybe, you started with the first as objective and ended up adding a couple of bullets about the second." I would not have been able to confess better. Maybe, I did that not so consciously.

The reason I am remembering and sharing with you all after all these years is that he gave me a justification. "If you have actually done that, I do not know how it would be evaluated by your journalism standards, but from our perspective, it is the right mix. Someone credible needs to do that."

I am not saying that what my colleague, Jatinder, has written in the cover story is actually a mix of 'woulds' and 'shoulds'. All I am saying is that, if you think so, I would be willing to still back the story.

Forecasting, and even if it is based on a structured survey of a large sample of respondents, is still not prediction. An astrologer can make prediction (not talking of accuracy; that is a dangerous area to tread into). An analyst or a journalist can make only forecast. The word itself means that it is an estimation.

The pandemic has proven how wrong all our forecast can go and how inadequate all our future planning can prove to be. All business continuity planning came to naught. But those who had a general sense of what the future would be – like more digitized business – could quickly figure out what they could do. If their businesses, this country and the world economy ran, it is because of their ability to 'do something' quickly. And that came neither because of detailed BCP/DR nor because these guys knew some magic. They knew the broad direction and they were good at thinking what could be done.

I would urge you to take the cover story like that. It is a general direction of where things will be in 2022. Some trends are already visible. Some could happen in 2023 or 2024, because of a number of parameters impacting them. It is not that they will be there only between 1st January 2022 and 31st December 2022.

What is important is to know where things may change; where actions need to be; and what is a broader direction.

So, take the story in that spirit. Since a lot of it has come from you all, some of it may sound familiar. If it gives you even one trigger point, our purpose would have been achieved. ■

NOVEMBER 2021
VOLUME 12 | ISSUE 08

Content

Cover Design:
ANIL VK

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

MANAGEMENT
Managing Director: Dr Pramath Raj Sinha
Printer & Publisher: Vikas Gupta

EDITORIAL
Editorial Director: Shyamanuja Das
Associate Editor - B2B Tech: Jatinder Singh
Assistant Manager - Content: Dipanjan Mitra

DESIGN
Sr. Art Directors: Anil VK, Shokeen Saifi
Associate Art Director: Shri Hari Tiwari
Sr. Visualiser: Baiju NV

SALES & MARKETING
Executive Director - B2B Tech:
Sachin Nandkishor Mhashilkar (+91 99203 48755)
Associate Publisher & Director - Community:
Mahantesh Godi (+91 98804 36623)
Associate Director - Enterprise Technology:
Vandana Chauhan (+91 99589 84581)
Head - Community Engagement:
Vivek Pandey (+91 9871498703)
Senior Manager - Community Development:
Neelam Adhangale

Regional Sales Managers
South: BN Raghavendra (+91 98453 81683)
West: Shankar Adaviyar (+91 9323998881)
Ad Co-ordination/Scheduling: Kishan Singh

PRODUCTION & LOGISTICS
Manager - Operations: Rakesh Upadhyay
Asst. Manager - Logistics: Vijay Menon
Executive - Logistics: Nilesh Shiravadekar
Senior Manager - Operations:
Mahendra Kumar Singh
Logistics: Mohd. Ansari
Head - Digital & Event Operations: Naveen Kumar

OFFICE ADDRESS

9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
121, Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091
Published, Printed and Owned by 9.9 Group Pvt. Ltd. (Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.) Published and printed on their behalf by Vikas Gupta. Published at 121, Patparganj, Mayur Vihar, Phase - I, Near Mandir Masjid, Delhi-110091, India. Printed at Tara Art Printers Pvt Ltd., A-46-47, Sector-5, NOIDA (U.P.) 201301.

Editor: Vikas Gupta

9.9 GROUP

EXTRA Curricular

A fine balace – cycling and sketching together give peace and happiness

The Joy Of Cycling

NEXT100 winner 2019 **Amol Bhandarkar,** Senior Manager - Solution Engineering, VMware shares his immense passion for cycling. He also highlights his love for sketching...

"I feel like an artist and my bicycle is the brush."
– Scott Stoll

I still remember the days when I was a kid and was introduced to the world of cycling by my father. Over the weekends, either on a Saturday or a Sunday evening, my father used to take me and my sister to Shivaji Park in Mumbai to teach us cycling. Cycling became my favorite pass-time. It was a need during my 10th grade to shuttle between classes. I lost touch with cycling post that year due to academics, thereafter work life took over. Recently, when I was told to add physical activity to loose extra flab, I recollected my long lost passion for cycling. For the past 8 years, I have been a regular cyclist, albeit I don't fancy myself going to 100+ KMs cross country circuit, like most of the cyclists do today. For me, 25 KMs on alternate days and 35KMs on a weekend are good.

Cycling taught me: Humility, Patience, Focus and Me Time. This hobby of mine has been picked up by my family too. My daughter, in particular, plans in advance to join me on a weekend ride either on highways or off-road in Aarey. During vacation, my family makes it a point to check if we can add cycling activity. In some cases, we have been lucky to have guided cycling tours off-roading through jungles, villages, farms (plucking fresh fruits), uphill-downhill across countryside contours.

Apart from cycling, sketching is one more such hobby that I have managed to nurture. As a weekend activity, I took to sketching to relax my mind by taking charcoal as a medium. Though not as a professional, but as an enthusiast, sketching has given me immense relaxation and capability to introspect. To sum up, I found a balance between cycling (a physical extracurricular activity) and sketching (an engrossing indoor activity). ■

As told to Dipanjan Mitra, Team ITNEXT

Amol Bhandarkar

Snapshot

Amol Bhandarkar is Senior Manager - Solution Engineering at VMware. He has been a NEXT100 winner in 2019. Bhandarkar was earlier associated with Automation Anywhere, Symantec, Microsoft, IBM India, etc. He completed his BE in Engineering from University of Mumbai and Diploma in Engineering (Industrial Electronics) from Bhausaheb Vartak Polytechnic.

Exploring new places, meeting new people and learning skills that help professionally

Explore The World!

NEXT100 winner 2019 Murali Lakshminarayanan, Director - Cloud Transformation, Capgemini Technologies, shares his immense passion for traveling and how it has helped him both personally and professionally...

"Travel makes one modest. You see what a tiny place you occupy in the world."
– Gustave Flaubert

Being a native of Kerala, brought up in Tamil Nadu, working in Karnataka and visiting multiple countries as part of the job, travel is an unavoidable element of my life. Thankfully, I am a person who always gets excited about traveling.

To me, traveling is not just about visiting a place and coming back. It is about exploring and experiencing the place where I go to. It also teaches a lot in terms of bonding with total strangers and instils self-confidence. This confidence has also helped me in my professional life to improve my communication skills and break the ice during conversations with new clients or prospective clients.

Among all the challenges that we faced during the COVID-19 pandemic; lack of travel was a key challenge too. It forced us to stay indoors. By God's grace, we have crossed the bridge thus far overcoming the COVID related issues. Currently, the overall situation in India is much better with lesser number of active cases and increasing number of vaccinations and vaccinated people. And after completing double vaccination, I started my travels following all the social distancing norms and hygiene rules.

A small waterfall deep inside a forest was my first travel when I restarted. This stands close to heart not just because it was very refreshing but also for the fact that the locals in the last village before the start of the jungle were so happy to see a new face after a long time. They offered hot coffee and food to our family and assisted us all the way till the waterfall deep inside the jungle by trekking for a few KMs. I must admit they were extremely friendly and cooperative and their knowledge of specific points in the area proved to be largely beneficial. In our beautiful country, I have to say, the gap between urbanites and people from remote areas is narrowing day-by-day, which is truly an amazing sign that augers well for the future of this great nation. India is well and truly shining!

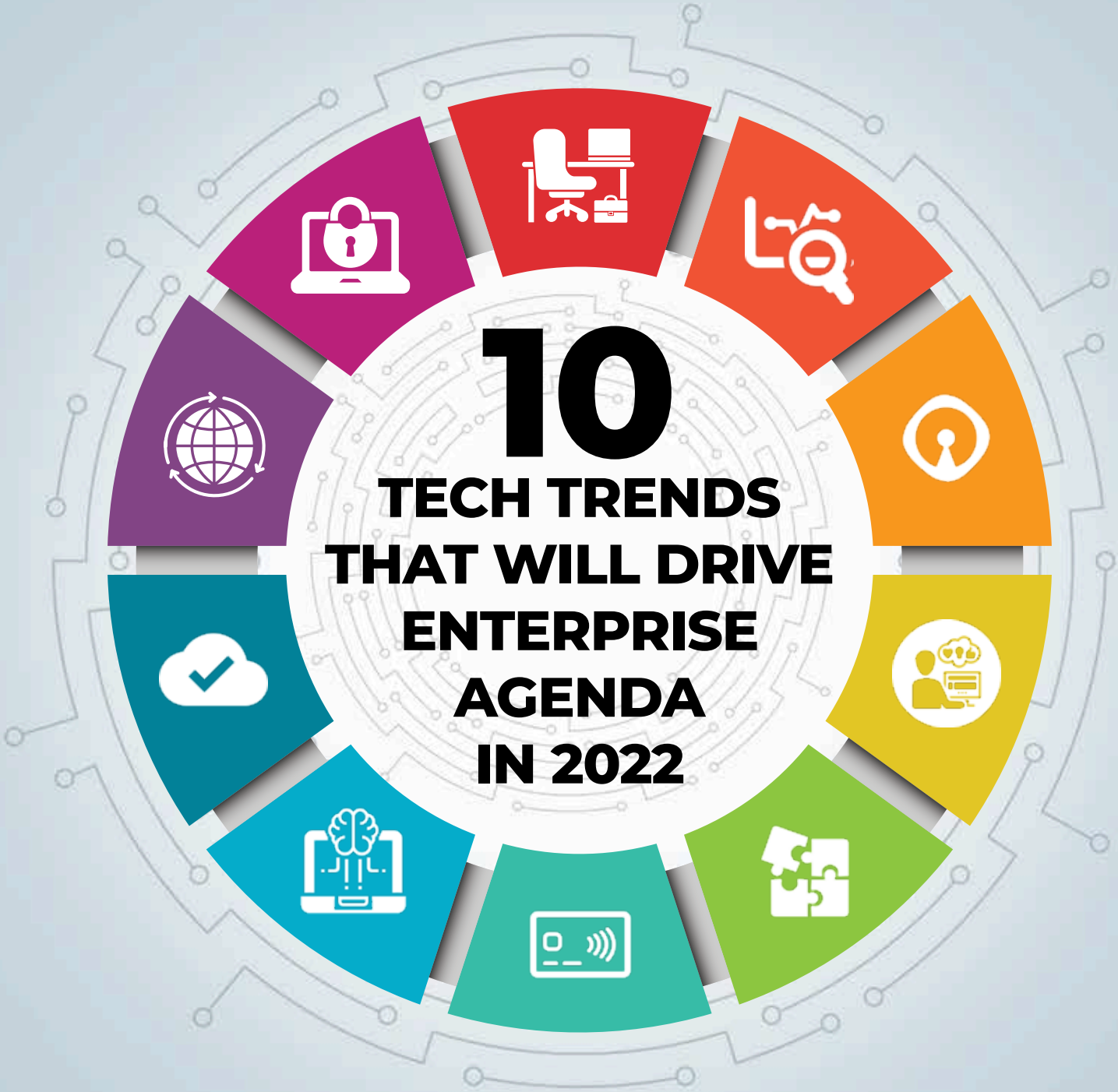
With the situation easing up and with everyone vaccinated, I hope the world becomes a safe place to travel again! ■

As told to Dipanjan Mitra, Team ITNEXT

Murali Lakshminarayanan

Snapshot

Murali Lakshminarayanan is Director - Cloud Computing at Capgemini Technologies. He has been a NEXT100 winner in 2019. Murali was previously associated with IBM India, Infosys, TCS and CSS Corp. He completed his BE in Electronics & Communication from Government College of Technology, Coimbatore.



10 TECH TRENDS THAT WILL DRIVE ENTERPRISE AGENDA IN 2022

Automation, predictive AI, cloud and edge-driven capabilities will empower organizations to adapt and reinvent in the new era of work

By Jatinder Singh

While the technology sector is known for driving frequent innovations and transformations, the last two years saw progress at an unprecedented scale. The global health crisis drastically altered the way we live and work. In the wake of a gloomy external outlook, the usual business operations and workplace models suddenly became archaic. The pandemic-induced work-from-home scenario resulted in a host of challenges businesses could've never imagined.

During the pandemic, IT leaders' first significant milestone was successfully enabling their entire workforce to connect, engage, and brainstorm by leveraging state-of-the-art technology and collaboration tools. Many new digital-centric enterprises rise to the challenge during turbulent times and launch unique business models by exploiting the advantages of the cloud, AI, robotics, and automation.

On the contrary, several organizations have continued to confront challenges related to managing erratic customer expectations, building supply chain resilience, and empowering a remote workforce to deliver exceptional user experiences during 2021. Many enterprises get exposed because of their complex business processes, which paused their ability to respond quickly to the change. While emerging technologies provided them with unique ways to solve these pressing issues, in several cases, the potential of these innovations could not be fully leveraged by businesses because of their low digital readiness index.

Overall, if 2020 pushed organizations to accelerate their digital transformation agenda to ensure business continuity, 2021 gave organizations realistic visibility around technology's role in augmenting specific processes.

As enterprises look ahead to the year 2022, they face a more significant challenge: how to continue to scale at lightning speed in the hybrid workspace environment, get back to business as pandemic subsides, and lay technical foundations for future-proof models.

There are immense expectations from CIOs and CTOs to continue leading this transformation and prepare bold action plans by identifying technologies that help organizations in their quest for success and disruptive business models.

Against this backdrop, IT NEXT has identified ten technology trends of 2022 that will likely form the agenda of enterprises to acquire novel capabilities, make their operations smarter, embed resilience, and deliver exceptional user experiences across touchpoints.

1. TOTAL EXPERIENCE (TX)

Delivering a better customer experience has been long considered as the foundation of the success of any organization. However, as digital adoption has taken a quantum leap across organizations and industries, enterprises need a new modern strategy to remain competitive and consistently drive exceptional customer experiences across all levels.

In 2022, a tremendous focus will be on revisiting business priorities and processes and finding technological solutions to make them more impactful to drive shared experiences that combine the disciplines of customer experience (CX), employee experience (EX), user experience (UX), and multi-experience (MX) will be highly critical for businesses. While CX, EX, UX, and MX get treated in silos in conventional business models, now the time is for more integrated approaches as enterprises expand to remote and distributed workforce environments.

According to Gartner, Total Experience (TX) is a business strategy that integrates employee experience, customer experience, user experience, and multi-experience across multiple touchpoints to accelerate growth. The total experience can drive more outstanding customer and employee confidence, satisfaction, loyalty, and advocacy through holistic management of stakeholder experiences.

Today, customers want the seamless opportunity to interact with multiple interfaces across mobile, web, app, and call. Businesses leverage new-age technologies such as AI-based chatbots, conversational AI, and virtual reality to connect with customers. Global Technology behemoths such as Amazon, Netflix, and Apple have already disrupted the customer experience by making their interactions with customers more meaningful and focusing on things that matter most to their customers.

In 2022, companies will continue to invest significantly in deploying multi-experience contact centers and purpose-built solutions relevant to their unique business models. One of the core boardroom agendas of CEOs will be to find the best ways to foster relationships between businesses and customers across all touchpoints by leveraging data science and AI/ML. Organizations will invest in tools and technologies that empower their employees to effectively map the entire customer journey and seamlessly resolve customer grievances.

"In 2022 and beyond, as the industry is moving towards colossal IoT adoption, edge analytics will be the cornerstone of enterprise strategy to drive connected ecosystems and innovations."

2. ON-DEMAND OFFICES

During the pandemic, businesses faced a considerable challenge to transition to remote work, to the cloud, and to accelerate digital transformation at a breakneck speed. However, getting their employees back to offices after COVID is even a more monumental shift that they are dealing with currently. 2022 will see a growing focus on in-person and remote work, aka, hybrid workplace scenario where enterprises will be rebalancing their real-estate portfolios and encouraging employ-

In Numbers

"AI, ML, Cloud Computing, and 5G will be the most important technologies in **2022**."
Source: The Impact of Technology in 2022 and Beyond: an IEEE Global Study

"In the next two years, **66%** of corporates expect to be making good progress on digital transformation."
Source: EY

"**86%** of buyers are likely to pay more for a better customer experience."
Source: Zonka Feedback

"The low code and no-code development platform market will grow to **USD 21.2 billion** by 2022, from USD 3.8 billion in 2017."
Source: Forrester

"By 2022, global AI software revenue is forecast to reach **USD 62.5**, an increase of 21.3% from 2021."
Source: Gartner

"**67%** of IT leaders believe that their workloads are set to significantly increase as IT becomes more an increasingly valued part of the business."
Source: Pegasystems and iResearch

ees to use on-demand workspaces. While some employees exhausted of work-from-home would happily resume offices, many others will resist, given the uncertainty around the future waves of the pandemic. And then, there would be a group of employees who want to work from the office but avoid the time, expense, and stress levels of a daily commute. This is where the concept of on-demand offices is likely to be an enabler.

On-demand workspaces are offices that are available when you need them without necessarily having a permanent address. In the new hybrid workplace scenario, where a significant percentage of total employees still expected to work from remote locations, on-demand offices offer unique advantages to employees who want to reduce their commute time without getting distracted while working from home. The concept also ensures that employees can meet their clients professionally without worrying about suitable space. Companies like We Work, Innov8, myHQ, and Regus are already offering unique office flexibility options and quality on-demand meeting rooms, training rooms, and workstations, even on an hourly basis.

The successful transition to the distributed work environment will need businesses to reflect on their technology readiness to drive the culture change, upskill people and ensure cross-departmental collaboration across their workforce seamlessly and securely.

Across all industries, there have been several experiments, tech integrations, process refinements, and new learnings to navigate the uncertainty and build capacities to support the distributed workforce model. Business leaders have to make subtle shifts in managing their teams remotely.

3. DATA AND ANALYTICS AT THE EDGE

As enterprises are flocking to the cloud more than ever today to reap the benefits of digitalization, the need for real-time data processing and analytics computation is expected to grow tremendously. By performing data analysis in real-time, at endpoints where it is collected, businesses across healthcare, financial services, manufacturing, agriculture, and transportation get empowered to make immediate decisions and deliver more incredible experiences to their users.

The edge analytics also enable enterprises to reduce the burden on backend servers while transporting computation and analytics capabilities even in remote locations. In 2022 and beyond, as the industry is moving towards colossal IoT adoption, edge analytics will be the cornerstone of enterprise strategy to drive connected ecosystems and innovations.

According to Six Trends in Data and Analytics for 2022, a report by Nucleus Research, as companies mature in their analytics strategies, most develop various priority levels for different analytical workloads as a means of optimizing costs and resource consumption, with the highest requiring immediate analysis and response and the lowest requiring very infrequent batched analytics or reporting.

The next few years will see growing demand for quick-to-deploy interfaces such as natural language to manage complex analyses and other workflows at the edge and within data repositories. "Keeping to minimize or eliminate latency, in-database analytics and query accelerators are seeing strong growth," the report adds.

4. LOW-CODE AND NO-CODE AUTOMATION

The adoption of drag and drop platforms, also known as low-code or no-code platforms, has seen significant interest across the industries during the last two to three years. In 2022, enterprises will continue to focus extensively on automating their processes and developing new customer interfaces by leveraging low-code and no-code platforms. The uptake is expected to grow sharply since these platforms offer the easiest way to establish modern-day applications and manage workflows, even when an organization lacks enough technical knowledge or resources.

These platforms enable businesses to amplify their capabilities by building responsive applications for mobile and web and cutting down the lead time between an application's coding and production state. Companies can automate processes and manage workflows even when they lack enough technical knowledge and resources by leveraging these platforms.

According to a projection by Forrester, the no-code development platform market will grow from USD 3.8 billion in 2017 to USD 21.2 billion by 2022.

An ideal no or low code platform enables the organization and IT decision-makers to achieve their business goals without compromising security. The winning no-code/low code technology strategy will require enterprises to carefully analyze which platform they want to commit to and whether they are precisely aligned with business goals.

"As enterprises look ahead to the year 2022, they face a more significant challenge: how to continue to scale at lightning speed in the hybrid workspace environment, get back to business as pandemic subsides, and lay technical foundations for future-proof models."

5. CONTACTLESS SERVICES

In 2022, businesses are expected to significantly accelerate their investments to offer contactless services across areas – delivery of products and services, customer experience, payments, and security.

Such measures will be critical to curtailing the risk of the COVID-19 pandemic to customers and

staff. The usage of robotics, AR/VR, and AI-powered applications such as facial recognition are likely to grow extensively in delivering contactless services such as telemedicine, education, dining, secure entrance to specific areas, and delivery of food & groceries. Innovations are likely to emerge in the augmented reality space where enterprises will demonstrate their products and services to customers virtually and in-store without physically touching them.

Last year, Tokyo 2020 saw phenomenal innovations in the contactless services space, numerous AR experiences, and live fan interactions and video messages for athletes for an engaging experience for athletes and audiences even if they are not in the stadium together.

In 2022, contactless payments will continue to be a preferred way of currency payments for customers due to the security, swiftness, and reliability it offers. "Contactless payments are beneficial for both consumers and retailers due to higher payments security, instant payment facility, low risk of theft, and high level of transparency. Furthermore, contactless payments witnessed significant growth during the COVID-19 pandemic as people started avoiding human touch to save themselves from infection," says a research study from Coherent Market Insights. According to the research, the global contactless payments market will account for 26.3 Bn in value by the end of 2027.

Technology enablers will continue to develop innovative ways to transform how we connect, collaborate, and get services effectively in a safe and contactless manner.

6. DEMOCRATIZATION OF AI & ML

It will not be wrong to say that if one technology has substantially disrupted the business processes, it is artificial intelligence (AI). So far,

"The successful transition to the distributed work environment will need businesses to reflect on their technology readiness to drive the culture change, upskill people and ensure cross-departmental collaboration across their workforce seamlessly and securely."

enterprises have only scratched the surface of the potential of AI & ML. In 2022, they will be the most critical technologies along with 5G and Cloud Computing. Almost all industries see AI as a considerable value creator in enhancing customer experience, automating processes, and firming employee engagement by leveraging data-driven insights.

The advancements of AI and ML enable businesses to predict future trends and make informed decisions to accelerate response time. For instance, well before the pandemic explosion, BlueDot, a Canadian AI-based health monitoring platform, observed some strange pneumonia cases in Wuhan, China, using natural language processing and machine learning. The platform alarmed public health officials of several countries even nine days before the WHO released a warning statement around novel coronavirus. The same AI platform also identified India and Brazil as future epicenters months before the second wave hit in these countries.

During the pandemic, concepts such as conversational AI-enabled contact centers provide round-the-clock personalized customer service and also help businesses bolster their supply chain efficiency even with limited staff availability. However, despite its insurmountable promise in terms of significant quality and cost optimization improvements, the mass adoption of AI & ML lags due to high complexity and talent shortage.

Tech-leaders are scrambling to find the right talent to accelerate their AI initiatives but cannot get from the existing pool of resources. In 2022, innovations are likely to emerge that will auto-

mate many AI initiatives, such as data groundwork and data engineering. The no-code and low-code platforms will be critical to democratize the AI within the enterprise ecosystems. Such tools will enable enterprises to integrate AI into applications easily, even if they lack talent who know the technicalities and science behind developing machine learning platforms.

7. UBIQUITOUS CONNECTIVITY

A poor network can be big detrimental to a digital revolution. Heading into 2022, the new hybrid workspace models require secure and ubiquitous connectivity to ensure employees and users can stay connected wherever they are.

In 2022, modernizing applications will be critical for enterprises to provide diverse choices for users to connect and collaborate with. Industry stakeholders in the IT and Telecom sector will continue to take strong initiatives to explore the potential of technologies such as 5G and WiFi-6 to create new IoT opportunities to drive better and secure user experience, even in rural and coastal regions. The improved connectivity could translate into incredible opportunities in public safety, intelligent transportation, smart farming, Industry 4.0.

Top Challenges for Technology Leaders in 2022

- Ensuring robust cybersecurity architecture for hybrid workforce
- Aligning IT investment strategy with business goals
- Managing return-to-office health and safety protocols, software, apps, and data
- Determining what technologies are needed for their company in the post-pandemic future is anticipated
- Recruiting technologists and filling open tech positions

Source: The Impact of Technology in 2022 and Beyond: an IEEE Global Study

"The no-code and low-code platforms will be critical to democratize the AI within the enterprise ecosystems. Such tools will enable enterprises to integrate AI into applications easily, even if they lack talent who know the technicalities and science behind developing machine learning platforms."

8. REGIONAL OPEN-SOURCE INNOVATIONS

While cloud-based applications are helping organizations provide a seamless experience to their

users across the globe, the rapid adoption of country-specific data-governance policies and standards are increasing the complexities. In 2022, as organizations continue to move to shared workplace models, they will be keen to analyze and learn from each other by leveraging on-prem platforms such as Azure.

There will be an extensive focus on region-specific open-source innovations and deployments to ensure compliance and find new paths to innovations. Various industry studies project that organizations with reliable open-source data stacks will be ahead of their competitors when driving revenues with data and analytics.

9. SOFTWARE-DEFINED BUSINESS CONTINUITY PLANNING (BCP)

A business continuity plan (BCP) outlines how an organization will run its operations during an emergency or an unexpected disruption. One of the foremost advantages is that cloud-based working models help create a compelling and agile business continuity strategy as compared with manually backup systems and traditional disaster recovery procedures.

In 2022, enterprises will focus on new software-defined strategies to back up their data and plan for disaster recovery should there be a crisis. Organizations will continue to invest heavily in skill up gradation and expertise to ensure that critical data, applications, and services remain operational or quickly reinstated if there is a disruption.

Investments in technologies such as containers and Kubernetes will likely grow faster to modernize the way applications are developed and leveraged to drive IT efficiency.

10. CYBERSECURITY MESH

The year 2021 has witnessed a significant improvement in information security awareness among Indian organizations. Nevertheless, driven by the rise in digital customer interface channels and the pandemic-induced remote-working, enterprises continue to witness new and unimaginable ways of cyber breaches throughout the last twelve months.

A report by Gemalto states that India accounts for 37% of breaches in the world that lead to stolen or compromised data. Security and risk management leaders continue to face challenges to secure sensitive and confidential organizational data. Businesses are deploying many technologies at numerous locations, and to protect their extended digital networks and digital assets, they need a planned and a new-age security approach. The year 2021 saw a rapid uptake of zero-trust network philosophy which makes all the devices by default untrusted to access the broader network. Zero Trust Architecture (ZTA) is a process that focuses on the 'do not trust, always verify' principle.

To keep pace with a more distributed workplace model and secure cloud deployments, industry experts are delving deeper into adopting the Cybersecurity mesh route, an extension of ZTA. According to Gartner, the cybersecurity mesh is a distributed architectural approach to scalable, flexible, and reliable cyber control. The mesh changes the focus from protecting a traditional IT perimeter (analogous to a "walled city") to a more modular approach that centralizes policy orchestration but distributes enforcement of cyber security policy. By 2024, Gartner projects, organizations adopting a cybersecurity mesh architecture will reduce the financial impact of security incidents by an average of 90%. ■

The Urgency Of Securing Evolving Workplaces

In the post-COVID era, the success of the new hybrid workplace model will be hugely dependent upon an organization's efforts in combining its digital transformation goals with robust IT security

By Ashok Kumar

The acceleration of digital transformation and increased cloud adoption has connected people, businesses, and culture like never before in recent times. In the pandemic-induced work-from-home scenario, companies have invested in data-driven technologies to stabilize their businesses and make their IT environments smarter.

The modified state of business priorities has been well-supported through analytics, automation, and artificial intelligence for enterprises. By embracing these technologies, enterprises have been able to mitigate unforeseen challenges and ensure business continuity remotely. However, this tectonic shift of traffic and rise in the remote working scenario has also compounded the network vulnerabilities, providing new opportunities for cybercriminals to expand their attack patterns.

By leveraging intelligence tools and exploiting the innumerable less-

secure end-points, cybercriminals have consistently launched novel attacks that are hard to trace.

Cybersecurity Ventures estimates that global cybercrime costs could grow by 15% per year over the next five years, reaching USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015. According to Purplesec, there has been a 600% growth in cybercrime-related activities in the last year. A survey conducted amongst 582 information security professionals found that 50% of the executives do not believe their organization is ready to repel a ransomware attack.

Massive surge in cyberattacks

Since the beginning of the pandemic, the industry has witnessed a significant rise in cyberattacks and data theft. According to a study by IBM, during the first three months of 2020 alone, India saw 37% more data breaches than in 2019. In addition, the country witnessed 16 million cases of cyberattacks, nearly three times that of 2019.

Driven by the exponential growth of data and the growing distributed workforce, cybercriminals are launching numerous malicious cyber campaigns loaded with pandemic-driven themes to trick the vulnerable distributed workforce. Various industry reports are testimony to that. According to Trend Micro, more than 60% of COVID-19-related threat detections came from the US, Germany, and France. The security firm also adds that despite being relatively new, the VPN vulnerability CVE-2019-11510 accounted for nearly 800,000 detections in 2020 alone.

RAH is seeing a huge uptake in demand of cybersecurity solutions by enterprises as well as organizations of all sizes in last few quarters, to be precise, since the beginning of the pandemic. WFH, increase in shifting to cloud, and other digital transformation initiatives have opened up plethora of avenues for cyber attackers. While these are timely and futuristic steps being taken by enterprises, cybersecurity remains at the core of all such initiatives.

In India, companies such as Air India, Dominos, Facebook, Juspay, Bigbasket, Upstox, among several other, have seen the critical data of their customers being stolen, causing a massive dent in their market goodwill.

Indian Computer Emergency Response Team (CERT-In) observed about 140 phishing incidents during the first half of 2021. According to CERT-In, fraudulent emails, SMS messages, and phishing websites pretending to be from legitimate services are reported luring users to divulge credentials to conduct frauds.

As more and more users are now using the internet for buying goods and services, hackers are also targeting the vulnerable population by sending unauthorized payment links and showcasing fake shopping websites. RBI has repeatedly issued a warning to banking customers that using these new tricks of unconfirmed SMSes and UPI notifications and unscrupulous hackers can wipe out the entire balance of banking customers.

Growing complexities

Among the biggest shocks in the cybersecurity space, SolarWinds supply-chain hacks of 2020 stood number one.

Fraudsters launched the attack by hacking the infrastructure of American IT Software firm, SolarWinds, and spreading malicious code to its over 30,000 clients through the software updates route. The worst part was that the list also included several US government departments, making their critical data open to cybercriminals. The attack reflected that most organizations are vulnerable to highly sophisticated mechanisms being adopted by the cybercriminals of the modern era.

It was also a cruel reminder cybercriminals are way ahead to create new channels to gain a foothold in enterprise networks. And even with robust IT security practices, organizations may not have enough ammunition to secure their networks.

According to the Infoblox Q1, 2021 Intelligence Report, in the instance of SolarWinds, the threat actor used a highly sophisticated attack chain to deliver malicious code through a backdoor injected into a dynamic-link library that was a part of a legitimate update to some versions of SolarWinds' Orion software. The report adds that the threat actor remained undetected for an extended time by employing sophisticated obfuscation methods such as imitating the legitimate SolarWinds coding style and naming standards. It did the damage by using Virtual Private Servers (VPSs) with IPs native to the victim's home country and leveraging compromised security tokens for lateral movement.

From a Domain Name System (DNS) perspective, Infoblox has been able to verify that once a victim has been infected with SUNBURST, the malware beacons to avsvmcloud[.] com with a hostname designed by a Domain Generation Algorithm (DGA) to exfiltrate data about the victim, as described above. The threat actor can return one of several responses in the form of an IP.

Due to the rapid uptake of remote work, organizations and employees have increased usage of collaboration tools, such as Meet, Zoom, and Slack. According to a Trend Micro report, the high use of these tools has led to the amplification of attacks such as Zoombombing, spam emails, and new ransomware variants that exploit these applications.

Many phishing attacks with COVID-19 themes are also getting noticed by the industry users where cybercriminals sent emails to users pretending to be senior executives from World Health Organization (WHO), tricking them to click on malicious links and documents.

Challenges aplenty

The majority of the security leaders still focus on reactive strategies

Factors such as upskilling and reskilling the IT talent pool, reviewing cybersecurity strategies, and build effective resilience programs will go a long way in developing a trusted environment. There have to be effective data security interventions

when it comes to IT security investments. While the current crisis has transformed that orientation a bit, most of the IT security initiatives revolve around traditional compliance and risk patterns. Another challenge that the industry has been battling for many years is the lack of cybersecurity talent. Due to the understaffed security staff, many organizations cannot leverage the capabilities of artificial intelligence, analytics, and automation when it comes to securing their workforce.

Going by Cybersecurity 2021 Part 1 survey report commissioned by ISACA and HCL Technologies, the last few years have seen massive demand for cybersecurity talent. However, due to low entry-level positions for the cybersecurity workforce, the industry has not created enough experienced talent pipelines in this space.

According to the report, 68% of the companies who experience more cyberattacks face a talent drought in cybersecurity, and 63% who experiences more cyberattacks historically are unable to hold qualified cybersecurity talent. In the age where AI, robotics, and IoT are taking center stage and making everything connected, lack of cybersecurity talent and poor governance practices can lead to more sophisticated attacks on enterprise networks.

In the next few years, the stakeholders in cybersecurity should come together to build a talent transformation consortium that can make a strong talent pool of cybersecurity talent.

With an extensive focus on remote working, organizations need to provide a secure IT environment to their people proactively. Factors such as upskilling and reskilling the IT talent pool, reviewing cybersecurity strategies, and build effective resilience programs will go a long way in developing a trusted environment. There have to be effective data security interventions, and they need to be well-supported by an in-house cybersecurity team and a strong technology partner.

In the absence of a well-carved IT security strategy, enterprises will find it really challenging to drive profitability and innovations in their business ecosystems. ■

The author is Ashok Kumar, MD, RAH Infotech

High Availability Clusters To Avoid The Real-Time Clutters

To alleviate system downtime and assure the high availableness of real-time servers, clusters are used

By Abhinay Deshmukh

To alleviate system downtime and assure the high availableness of real-time servers, clusters are used. Clusters are groups of various servers that are mapped and worked together and participate in workload management. A cluster can contain number of nodes and other application servers. A node is basically a physical computer system with a different IP address that is running one or more application servers. It means that multiple servers are grouped together to achieve the same business and can be regarded as one computer. Logically associates many servers and clusters with different configurations in their organizational environments.

Clusters and Workload Management

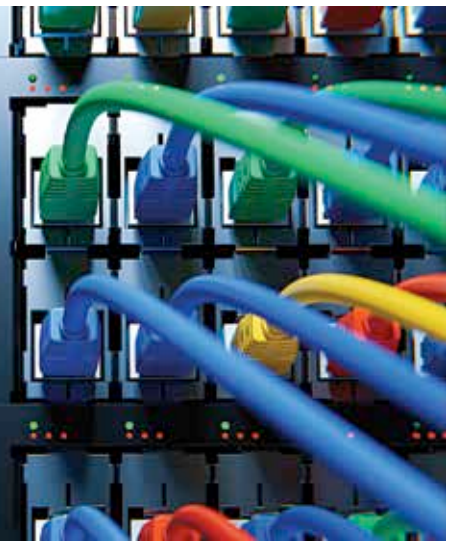
While implementing the data center and the server management system for a huge enterprise that gets more than thousands of transactions per minute, the most important thing in that design is the "Clusters of Servers". At least 2 servers with high and excellent quantity of memory must be

clustered in a data center for every module or logic so that we should not face a situation of a deadlock resulting in all the messages getting cluttered in a queue. In the article, we will see some of the benefits of clusters and how they are formed and if clusters are not there, then what issues can arise for the enterprises.

The clusters do a very important job in solving many complex issues related to the software, hardware, network, memory, time, and location. You might be wondering sometimes, how clusters solve such important issues. The magic lies in the architecture in which the clusters are created and managed. The data centers mostly form the most important hardware location and mostly those are found centralized at one headquarters or at one place getting connected with various clients and various locations throughout. We can then fetch the data from and to servers. This setup of servers is common to solve the client-server technology, but in our enterprise where there is n-tier architecture with a client and various servers, starting from the technical files server, business logic files server, and the database servers, we must connect all these in a line to get the work done. Then to have the flow continuous without any stoppage, we must introduce clusters into server architecture.

Clustering or a server in a data center makes a server more robust and stronger to communicate with the databases, the messages in the queue, the clients, which can do the transactions in the real-time as well as in batch saving and utilizing time as needed. Clustering a server is the most important design pattern of a server that makes a server more powerful by creating high availability, a tough load balancer, and a directing agent of the messages to a particular node of a server checking how much data can a server-node manage and how much time will it take to process a functional data.

The clusters do a very important job in solving many complex issues related to the software, hardware, network, memory, time, and location. You might be wondering sometimes, how clusters solve such important issues



Clustering is an integrator of a data servers that divides the data into different nodes. This sort of design eases the hardware and its setup making it convenient for the hardware engineers to maintain it as there will be hardly any emergency required since if one node goes down the second node will take over and vice-versa. The software programmers accessing the server won't face any issue such as down time or the server not responding which can go a long way to achieve the confidence of the team who is entirely dependent on working with these servers.

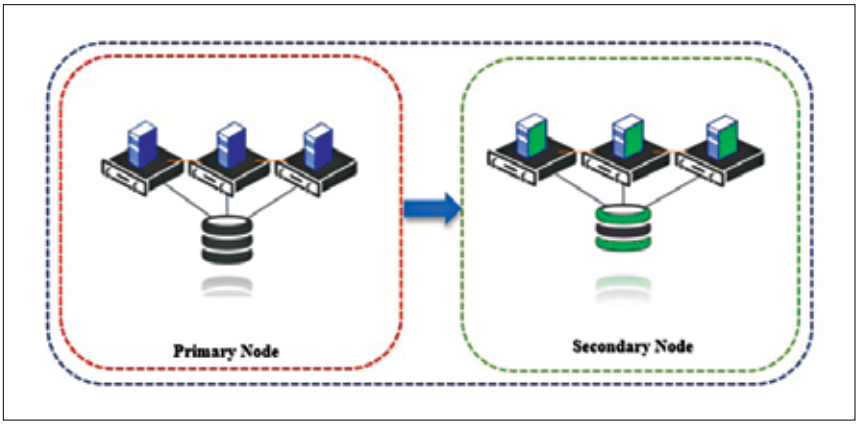
Types of Cluster Computing

Computer clusters can generally be categorized into three types:

1. Highly available or fail-over
2. Load balancing
3. High-performance computing

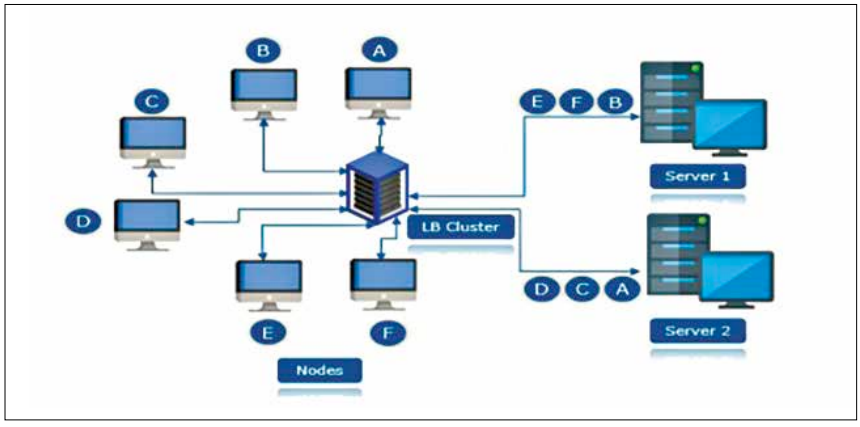
1. Highly Available or Fail-over

High Availability (HA) clustering is a method used to reduce downtime and provide end-to-end service when certain system components fail. Highly Available clusters consist of number of (multiple) nodes that exchange the data and information through the grids and as a result, it is an efficient and robust way to ensure high system performance, availability, reliability, and scalability. The basic principle in this category of cluster is that if a case one node fails, then server applications and utilities can be made available to other nodes.



2. Load Balancing Cluster

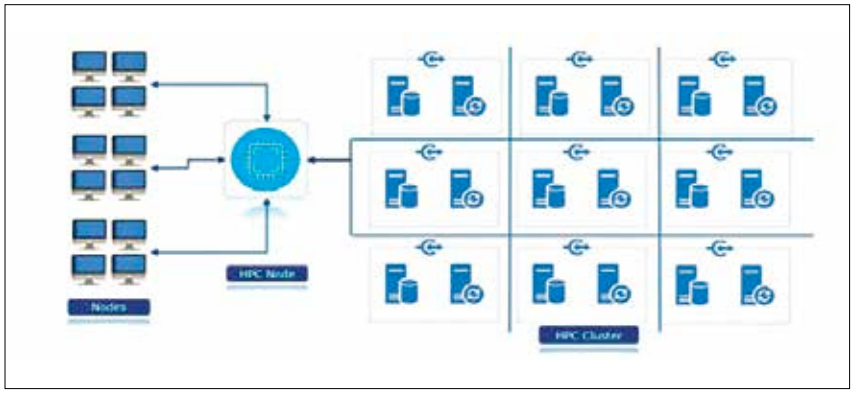
Load Balancing Cluster allots all the incoming requests from various nodes towards the load balancer. By using certain advanced algorithm, all the requests and load is divided into multiple sub tunnels. In this Cluster model, all the server nodes are responsible for tracking orders, and if a node fails, then the requests are distributed amongst all the nodes available.



This typically works to manage the server workload so that it is evenly distributed among the multiple parent servers. The load balancer cluster monitors each server and divide the workload according to a predetermined formula or algorithm.

3. High-Performance Computing

A High-Performance computing cluster consists of number of computer server systems that are connected.



Each server is called a node. The nodes in each cluster work in parallel with each other, boosting processing speed to deliver high performance computing.

High-Performance computing cluster plays an important role, in multiple industries and functions. In this type of cluster where thousands of computers servers use parallel processing to achieve higher computing power than could be achieved using just one of the computers in the cluster. A small cluster may use as few as four nodes, and a large cluster may have thousands of nodes. (A supercomputer has thousands of nodes, for example.) Regardless of how many nodes there are, multiple nodes use the power of parallel processing.

Advantages of Server Clustering

- **Performance:** Basically, measured as the response time, and turn-around time to perform several complex tasks with number of virtual machines at the same time. Clusters generate higher levels of performance.
- **Availability:** Clusters provide zero interrupted services by scheduling and distributing the complex work, or through shifting the application services to surviving nodes by way of a failover process.
- **Scaling:** Clustering servers is completely a scalable solution. You can add number of other resources to the cluster afterwards. Clusters have the ability to add capacity as needed and also flexible with the new technology configurations.
- **Manageability:** If a server in the cluster needs less maintenance, as there are number of advance applications which can triggered and continuously sent the statistics reports for the networked clusters. Clusters have the ability to be managed as a single system and restart and troubleshoot easily.

The server clustering concept ensures the round the clock availability to the online businesses and robotics environments even if there are some major issues going on with a server within the cluster. The server clustering is a successful solution implemented in many web hosting services, despite the fact that it has also some limitations. Also, when the clustering concept is applied to a project, the team gets free from continuously monitoring the availability of the servers and also, they get more time to think of more important solutions and manage the servers more efficiently. The additional tasks can be added in the servers like creating more parallel programming and scheduling of the jobs. The monitoring and the debugging of the cluster of servers more effectively since the fundamental things are sorted when we form the clusters. ■

The author is RPA Consultant at Atos India

Formulating Robust Protection Plans With Endpoint Security Top Of Mind

Administrators need to ensure managed endpoints are running the correct version of the installed security software components, as mandated by compliance policy

By Debasish Mukherjee

The pandemic has changed the way businesses work and the way IT secures them. Now, more than ever, organizations must have solutions to manage and secure all endpoints. With end users logging on and off the network using devices with unpatched vulnerabilities and with encrypted threats reaching endpoints unchecked, devices must be secured for the safety of both the endpoints themselves and the network. As ransomware and credential theft become increasingly more pervasive, endpoints have become the battleground of today's threat landscape. Despite a wealth of solutions in the market,

administrators still struggle with the visibility and management of their security posture. Additionally, they are challenged by having to provide consistent assurance of client security, along with actionable, easy-to-use intelligence and reporting.

Here are some of the drawbacks of Endpoint Security that organisations may encounter while formulating protection strategies:

Redundant Security Solutions

Administrators need to ensure managed endpoints are running the correct version of the installed security software components, as mandated by compliance policy. This issue is exacerbated when dealing with traditional antivirus solutions that rely on an updated signature database to defend against the latest threats.

Advanced Endpoint Protection (AEP) solutions that work by examining system behaviour (heuristics) perform better against these attacks and can also block malicious scripts such as seen in fileless attacks.

Policies and Web Compliance Enforcement

Administrators struggle to mitigate the risks that come with people using their devices on third-party networks at home, in coffee shops, at hotels or at airports. At the same time, they face challenges when it comes to enforcing the company's web usage policy away from the office. Outside the workplace, people are more likely to hit malicious web properties and tend to visit productivity-wasting websites. And if your users are pulling all their data through your data center via VPN, bandwidth-intense content such as video may need to be throttled.

Throughout the early days of the pandemic, network administrators complained that their networks were being inundated by TikTok, YouTube, Netflix and other traffic from streaming services and this problem will continue to grow as picture quality improves and people increasingly rely on these apps for entertainment.

Getting Reports and Managing Access

In some cases, administrators may manage multiple tenants through firewalls, but their users are configured in a single pool. This makes obtaining a single sign-on (SSO) from a firewall admin or security management consoles a challenge when trying to manage client policies. At the same time, compliance regulations often dictate that all admin roles adhere to the principle of least privilege, so a unified client management suite that can't manage role-based access controls will cause numerous headaches. For example, someone may be limited to two roles, one which has read/write access and one which is read only access.

Encrypted Channel Threats

With more web applications being secured through encrypted channels like HTTPS, and with malware also resorting to encryption to bypass network-based inspection, it has become imperative to enable Deep Packet Inspection of SSL/TLS traffic (DPI-SSL). However, this is not easily enforced without the mass deployment of trusted SSL/TLS certificates to all endpoints to avoid user experience and security challenges.

Understanding Alerts and Remediation Steps

End users are typically less aware of security risks than security professionals and as such, they don't understand the alerts on most endpoint security clients. In addition, most clients don't include self-help information, which results in users either ignoring the issue or filing tickets with IT. For example, if a user's device falls out of policy and that user is quarantined, that user won't know what is required to get back in compliance.

License Management

One issue on the backend of endpoint security software is that administrators, particularly when it comes to MSSPs, can't ensure their software is licensed correctly. If license information related to customers isn't centrally monitored and stored, it could cause outages and gaps in security. Additionally, administrators may struggle to run compliance reports against all deployed third-party licenses to pay their partners.

Stopping Advanced Threats such as Ransomware

Traditional endpoint security approaches can sometimes leave gaps in meeting administrative requirements. The long-embattled signature-based approach of traditional antivirus technologies has failed to keep pace with the development of new malware and malware evasion techniques. Many legacy solutions fail to deliver advanced threat detection and lack support for a layered defence strategy on endpoints, including integration with a sandboxing environment.

Not Knowing Where Critical Vulnerabilities Lie

With the large growth in business applications, the threat of application vulnerabilities has increased exponentially causing headaches for IT administration and resulting in breaches. Many organizations still don't have a way to identify the number and classification of vulnerabilities, which makes it difficult to create a plan for either patching or uninstalling risky applications.

While the number of potential pitfalls may make formulating an endpoint protection plan seem impossibly complex, there are plenty of resources available to simplify the process. With so many endpoints potentially connected to an enterprise network at any given moment, organizations need greater visibility and control, as endpoints are a common entry point for malware and other attacks. Security administrators need to evaluate the various endpoint solutions available with real-world requirements in mind. ■

The author is Vice President, Regional Sales - APAC at SonicWall

Need For CXOs To Move From Product To Platform Mindset For Intelligent Business Solutions

Platforms harness the power of multiple revenue streams, pervasive customer insight or data and creators' possibility to build more layers of innovation on top

By Anupam Kulkarni

Digital platforms have become an absolute must for any business and are no longer a digital native strategy. According to a popular survey, "platforms are quickly becoming a must for competition and a foundation for creating new value — and companies that fail to embrace them might get left out on the sidelines by watching them." Many digital platforms have become an integral part of the business landscape and are no longer exclusively digital natives' domains.

In the Age of Platforms, the term is almost a buzzword in the industry. Tech giants like Facebook, Apple, Google, and Amazon have redefined business, a platform that is merely a structure made up of integrated features. For example, Amazon initially was an e-commerce delivery platform. Adding integrated features like AWS, Audible, Amazon Pharmacy, Amazon Fresh, and others have shifted from a product to a trustworthy platform.

Likewise, Google, which was initially a search engine, has now adding planks such as YouTube, Docs, Maps, Gmail, and others have turned into a platform.

Platforms harness the power of multiple revenue streams, pervasive customer insight or data and creators' possibility to build more layers of innovation on top. When Amazon struggled to achieve scale as a singular e-commerce business, they turned inwards to seek a more solid platform, systems and processes. That laid the foundation for the world's largest cloud service provider. Companies including Daimler, Nike, and Unilever are launching their platforms as their business models mature. Effective platforms are based on technological excellence but cannot exist exclusively in the technical realm. They rely heavily on support and feedback from other parts of the business that are coordinated better through a cross-functional team that defines success metrics and tracks progress. Centralized leadership by the CXO can manage this better by mobilizing the right talent and "product owners" accountable for success in their specific business areas.

Need to move from product to platform mindset

Developing a business platform strategy requires slightly different products to help entrepreneurs and managers create and capture value. Companies that focus on building platforms have learned to integrate an ever-widening universe of partners and consumers into their ecosystems. Consumers rather than enterprises drive today's economy—the need for CXOs to focus on consumer-driven platforms matters more than ever. Many products have transformed into software as a service. For instance, Microsoft's traditional "Windows First" strategy evolved into the "Cloud First or SaaS" model with emerging technologies. The company recognized that transformation was not just a strategy by mindset about the customer experience and sales function.

Leaders must rethink the shift from transforming products into services while considering what services instead of products across industries. All companies face limitations when it comes to driving innovation. However, it is possible to expand those limitations with a powerful platform. Innovation is the responsibility of every stakeholder in the company, making it a contribution by partners, users, developers, and other collaborators. Building a platform gives the power to cultivate the whole ecosystem. The development of digital media assisted by the third-party API (Application Programming Interface) providers can allow participants to exchange data for developing new services. The main goal of digital platforms is to improve collaboration between end-users and manufacturers to transact with each other. These platforms allow users to exchange various information, such as new products and services and connect the platform's ecosystem. This technology also makes it possible to build a reliable network to add value.

How is the platform strategy beneficial?

Platforms shift knowledge ownership from the owner to the community & personas using the platform. Platforms are built for catering to different personas with different needs, which in turn means aggregation of different data sets. The handling of data of a platform needs to be well thought out, as otherwise the true potential of any platform will be left uncovered. The ability of a platform to break data-sets into bite-size, actionable insights that an enterprise can use to get better, deliver better experience and identify opportunities, binds the entire organization together. The biggest power of a platform is to reduce 'data' silos and aggregate data sets which enable cross function/teams valuable insights for successful use-cases.

What is a platform strategy framework?

The digital platform strategy aims to penetrate the online marketplace, focusing on allowing one segment of participants to benefit from the presence or interaction of others. The general assumption is that customers can independently determine their willingness to pay for a service or product. However, platforms can disprove this assumption, as the participation of the user segment on the platform depends on the user's choice. Developing a business platform strategy requires slightly different products to help entrepreneurs and managers create and capture value.

Digital platform strategies need to align well with the organization's work across all channels. If they are not well integrated, businesses will often run into problems in the long run. To develop an effective platform strategy with long-term solutions, collecting as much information as possible is essential. Along with this, define goals and criteria from the very beginning. The use of digital platforms in the workplace has become commonplace. Platform strategies, whether practiced individually or jointly, become a strategic imperative. Companies that have yet to make the transition will find it challenging to keep up.

Platform companies move faster than their product-centric traditional counterparts. The post-pandemic time is crucial to expand one's horizons, and platforms help to diversify with intelligent business solutions while reducing the risk. The CXO needs to dematerialize a traditional ecosystem and aggregate functions on a platform. It has been assumed for a long time that leaders need to commit resource allocation and operations to either product-based or platform-based approaches. However, moving away from the traditional strategy, companies have successfully transitioned from product to platform and have employed a hybrid model. ■

The author is CEO & Co-Founder, iauro Systems

Optimizing Organizational Downtime And Empowering Employees In Hybrid Workspaces

A long-term vision is needed to build a robust hybrid workplace strategy for the future

By Rajiv Bhalla

Ashish, who completed B. Tech in Computer Science during the pandemic, got a dream offer from a Bangalore-based startup. Thanks to efficient collaboration tools, he was on-boarded following a series of interviews and interactions with the HR and top management. As some of his team members are located across the U.S. and India, he opted for a flexible work schedule to ensure he attends pre-scheduled weekly meetings and weekend reviews. With things getting back to normal, the organization asked employees to decide which work model they preferred – on-site or remote, and they unanimously opted for hybrid work.

The hybrid model offers the best of both worlds

Increasingly, employees are choosing the flexibility of working on-site and remotely for parts of the week. The hybrid model is finding favor with a lot of organizations and employees. For digital organizations, the model delivers multiple benefits. Firstly, employees receive the flexibility to work across different schedules, as seen in Ashish's case, wherein he is required to collaborate with team members in varying time zones. As many IT organizations also have clients abroad, it becomes feasible for them to allocate employees in different shifts and allow them to work from the convenience of their homes. Office visits are reduced to half or one-third of the prior commitment, saving a considerable amount of employees' time and resources.

A flexible approach creates opportunities to optimize investments and implement innovative ideas across the workspace environment on the business front. For example, the savings in infrastructure, logistics, and utilities realized through remote working can be directed to employee welfare activities like health insurance and holiday programs which will motivate the employees to do better and remain loyal. It will also help reduce attrition and enable cost efficiency across the entire value chain.

Increasingly, employees are choosing the flexibility of working on-site and remotely for parts of the week. The hybrid model is finding favor with a lot of organizations

Meeting the demands of both models

Employees working from home will also have to fulfill their roles at home; this may lead to conflicts and directly impact productivity. In such an ecosystem, businesses must adopt strategies to optimize employees' time and manage organizational downtime. Collaboration tools can help organizations in keeping employees engaged and satisfied at work.

Modern collaboration suites open up infinite possibilities for a hybrid model. Meeting, messaging, polls, whiteboards, virtual events, and social networking – all of these can add value to the workspace. With automated, AI-driven features, employers can also get insights into the moods and motivation levels of the employees during meetings and other routine engagements. By understanding employees' engagement patterns and identifying the pain points at various levels, organizations can devise strategies to improve their well-being and motivate them further. Collaboration tools with multiple language support, intelligent features to combat video fatigue, and advanced background noise elimination technology are among the few that can enhance the overall experience.

Creating and sustaining the long-term vision

Now, with hybrid workspaces becoming a crucial part of the digital culture, organizations need to create and sustain a long-term vision to make it a decade-long reality. With technology laying the foundation of this strategy, organizations need to be prudent in their investments. Adopting the right technology with sufficient room for scalability and flexibility is of paramount importance. Security and data privacy are essential aspects to consider while sharing the organization's IT assets across the entire employee network, not just domestic but international. Thus, there is a need to build a robust technology platform and customize it with the right tools to facilitate improved collaboration and security. Depending on the nature of work, organizations may have to add custom tools to optimize employees' time and capabilities. Some examples are integrating a call center software suite for homebound employees and implementing analytics software for marketing/insurance categories.

It is also essential to equip employees with shared facilities, as provided in brick-and-mortar scenarios. Most of the businesses have started allocating special funds to meet these demands. While giving employees monetary incentives for Internet access, PCs, software, and educational apps, the organization should also ensure that employees effectively utilize the funds. Managing and monitoring all resources, including the software and physical assets, is vital to ensure the effective functioning of the hybrid workspace. ■

The author is the Managing Director at Barco India

Addressing WFA IT Pain Points With SD-WAN And ZTNA

Work From Anywhere model requires seamless access to business-critical applications and data both on-premises and in the cloud, regardless of where the user accesses them from and this must all happen without compromising network security

By Rajesh Maurya

During the pandemic, transitioning to a work-from-home model required organizations to move critical resources to the cloud, ensure employees had access to essential business applications, and secure communications between the home office and corporate network. And now, instead of moving everyone back into the corporate office, many organizations are transitioning to a work-from-anywhere (WFA) approach, with some employees working from home, others on-site, and others spending part of their time in each location.

This new approach provides much-desired flexibility and improved work-life balance for workers, increasing productivity and work satisfaction.

Companies also realize several logistical and financial advantages that come with reducing corporate office overhead. But accommodating this hybrid workforce also requires networks to become hybrid while still being able to balance security with user experience.

Quality of Experience and WFA

Quality of Experience (QoE) measures how satisfied workers are with their entire work experience. It includes ease and speed of access to essential resources, consistent availability of business-critical applications, and quality of service for things like voice and video conferencing.

But maintaining QoE for a WFA workforce is a challenge. It requires seamless access to business-critical applications and data both on-premises and in the cloud, regardless of where the user accesses them from. Further, this must all happen without compromising network security, which is particularly challenging considering that home networks and remote devices are notoriously under-secured.

Three Key IT Pain Points in WFA Models

Ideally, accessing corporate applications and data from anywhere should be seamless, but remote connectivity often impacts the user experience and security posture. Resolving these issues requires addressing three key IT pain points.

1. Unpredictable Experience

A common approach to maintaining security while handling remote traffic is to backhaul all application and internet traffic through the corporate data center for verification before reaching its destination. However, this increases latency and wastes bandwidth compared to a direct connection. Such architectures can also be complex and expensive to operate because IT must individually configure and manage branch routers and stitch firewall policies.

Quality of Experience (QoE) measures how satisfied workers are with their entire work experience. It includes ease and speed of access to essential resources...

QoE becomes inconsistent for branch end-users because backhauling application traffic can impact application reliability. Home users are forced to access applications through a VPN tunnel to the corporate network, leading to even more unpredictability due to variations in home bandwidth capabilities.

Challenges remain even when organizations allow direct access to cloud applications because improved application experience comes at the cost of security. Home users must also still use a VPN to access internal resources, making their overall experience inconsistent.

2. Inconsistent Policies

IT teams find it challenging to ensure consistent policy enforcement across the network when different sets of security are deployed on-site, at the branch office, in the cloud, and at home locations. This is because an overall lack of visibility and control creates a landscape ripe for threats to leak through. In fact, threat researchers have recently detected a shift in threat actor behaviour aimed at exploiting policy inconsistencies by targeting home or smaller branch offices rather than attacking traditional network devices. These bad actors can access a device deployed in an under-secured network and use it to hijack a VPN connection back to corporate resources, rather than having to force their way past commercial-grade security.

3. Implicit Trust

Many organizations use an implicit trust model when providing access to applications. Those using a VPN connection are usually authenticated with a generic process that provides access to the entire network, with the assumption being that any device connecting through a secure VPN tunnel is to be trusted. But all it takes is for a remote user's machine, identity, or credentials to become compromised for an attacker to ride that trusted VPN connection to gain access to the entire network.

Meeting WFA Challenges with SD-WAN and ZTNA

When implementing a WFA model, organizations must adapt their existing infrastructures and security models –traditional security and connectivity solutions are simply not up to the task. The good news is that the challenges described above can be met with the deployment of Secure SD-WAN and Zero Trust Network Access (ZTNA) solutions.

While SD-WAN is great at providing reliable connections to cloud-based applications, most SD-WAN solutions lack integrated security. In contrast, Secure SD-WAN on a purpose-built security platform blends advanced connectivity with enterprise-grade security and allows for single-console management, enabling consistent policy creation, deployment, and enforcement. Further, ZTNA provides per-user access to specific applications, far surpassing implicit trust when it comes to security. Every device, user, and application can be seen and controlled regardless of where they are connecting from. Together, solutions like Secure SD-WAN and ZTNA help businesses meet the challenges and realize the opportunities that WFA provides. ■

The author is Regional Vice President - India & SAARC at Fortinet

Trend Forecast For 2022: How Will Video Analytics Technology Change The Industry?

Usage of video analytics enables businesses to generate highly actionable data from vast volumes of video and preserve only this information instead of storing several terabytes of video footage generated by the cameras

By Abhijit Shanbhag

We are living in a world that is increasingly becoming technology dependent for almost every need. With the arrival of CCTV-enabled centralized monitoring, the need to rely exclusively on the deployment of human security personnel was eliminated. And now, video analytics technologies are enabling preventive vigilance as well as quick investigation, identification of criminals and resolution of incidents such as trespassing, burglary. Today, video analytics evolution offers ample scope for global transformation across industry verticals.

There are billions of cameras deployed for surveillance purposes all over the world. Add to it another billions of cameras fitted into the

smartphones and other personal devices, and we have a mind-boggling ecosystem that is generating unimaginable volumes of video data every minute. Integration of AI analytics with machine learning is now bringing to fore novel ways of utilizing this video data that stretch far beyond the good old security needs that the CCTVs were expected to meet. Video content analytics is being used in a number of ways in modern smart cities. Traffic and crowd management, video surveillance, retail store management for better customer experience and remote monitoring of contagion patients in healthcare facilities are some of the prime use cases.

However, new trends are rapidly emerging on the block. The video analytics platforms are being embedded with the conventional CCTVs to add abilities such as object and facial identification, analysis of image data captured from videos, and edge analytics at the camera end that eliminate the need to transfer data to the central server for analysis. This results in reduced bandwidth usage and enhanced speed.

Future of video analytics

Analytics is a rapidly evolving technology and with advancement of AI engines, the video data can now be used as a basis for predictive analytics and forecasting future market trends, patterns, and behaviors which help make the surveillance system increasingly intelligent and capable of taking decisions.

Video analytics trends indicate that the technology has barely scraped the surface of its potential as well as deployment so far. With further surge in IoT and cybersecurity demand, advanced video content analytics will be adopted at a much faster rate. The eventual merger of advanced video content analytics with cybersecurity tools will open up a whole new vista of opportunities.

Usage of video analytics enables businesses to generate highly actionable data from vast volumes of video

Analytics is a rapidly evolving technology and with advancement of AI engines, the video data can now be used as a basis for predictive analytics...

and preserve only this information instead of storing several terabytes of video footage generated by the cameras. The likelihood of human error is also reduced when the video AI technology is used to identify different actions, objects and behaviors.

Another rapidly growing aspect of video analytics is in the form of smartphone apps. It is possible to use mobile cameras in sync with video analytics in various processes. In health and fitness, we are witnessing how video analytics is helping people improve their workouts courtesy of motion capture and analysis features.

Video analytics technologies are already being used in various functions such as:

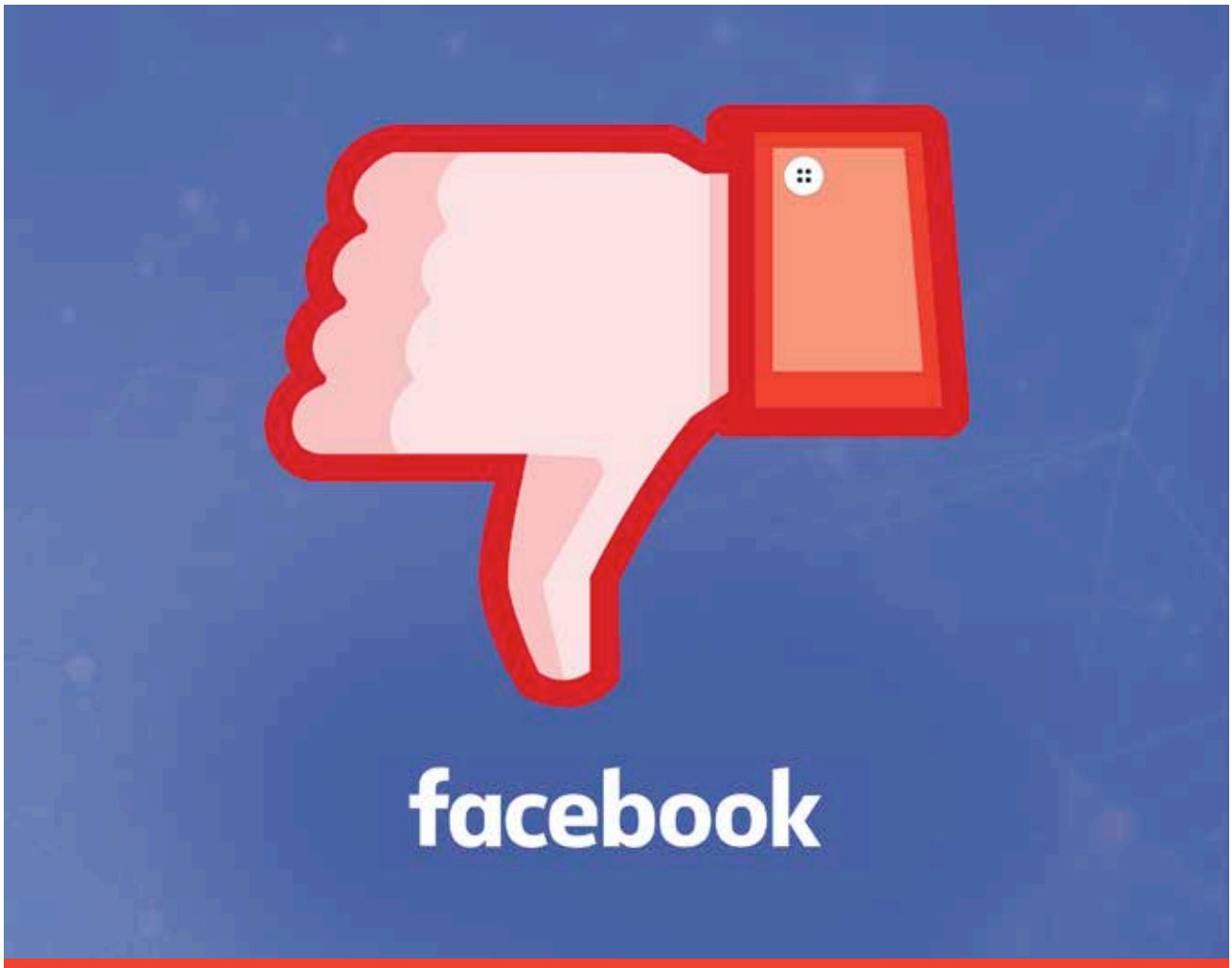
- **Detection and tracking of objects** – Unidentified objects lying at an airport or haphazardly stored items on a store shelf, it is possible to identify and track objects throughout monitored premises through the technology.
- **Motion tracking** – Integrated image sensors, night vision and other tools enable video analytics usage for purposes such as speed tracking of vehicles to intrusion monitoring on perimeters.
- **Facial recognition** – In the arena of security, video analytics has great potential courtesy of facial recognition features. Monitoring of people, spotting unusual behavior as well as identifying criminals from an integrated database are some of the things that can be done.

It is due to these advanced features and analytical capabilities that finds utility in various business verticals such as the following.

- **Sports and event management:** Using video analytics in sports has been around for quite a while. Coaches and analysts use video footage of players to understand what they are doing and how a player's actions are impacting his/her as well as the team's performance. For instance, monitoring a footballer can help a rival coach to understand his strategy and advise his team to counter it. In event management, the technology can be used to monitor attendees and take steps to enhance their experience.
- **Retail:** Video analytics is proving to be a pot of gold for retailers as it enables generation of crucial insights about customer behavior that regular data analytics isn't capable of. Creating heat maps of the customers makes shopkeepers identify their best performing and worst performing products and aisles and lead to optimisation and improvement of the customer experience.
- **Healthcare:** Observing patient behavior, perimeter surveillance and monitoring of patient vitals remotely are some of the things that video analytics can facilitate in healthcare. Doctors can safely monitor and advise multiple patients without the need to risk visiting each patient in-person especially in times like these when there is a heightened risk of infections.

There is no doubt that video analytics has now opened the door through which we can overcome human limitations and eliminate human errors. The technology is becoming increasingly responsive and useful with the evolution of video cameras and AI-powered image capture technologies. Trends indicate that video analytics will play a role in almost every aspect of life in 2022 and beyond. ■

The author is President and CEO, Graymatics



What Enterprises Can Learn From The Extended Facebook Outage

A recent blackout of Facebook and its associated services for six hours created massive chaos among users and pushed businesses to reflect on alternate real-time collaboration methods

By Jatinder Singh

Recently social media giant, Facebook, and its associated services Instagram, and WhatsApp, suffered massive outages that halted its services for almost six hours at a stretch and sent many in a frenzy. The users could not send or receive any messages and were unable to make or receive calls either. Facebook had earlier experienced a prolonged outage in 2019 when its services and applications were down for about 24 hours.

While lengthy outages of technology companies are not unusual, they could create massive chaos among users due to the unprecedented digital-first environment we have recently transitioned into. The event also demonstrated our excessive dependence on a single company to connect and collaborate with colleagues and families in real-time. Facebook's top-notch IT talent's failure to resolve the issue promptly or the absence of a solid backup backbone strategy to get things moving is a concern that the social media giant would like to address.

The disruption caused a dramatic impact on the fortunes of Facebook's share market appeal, where its stocks dropped significantly by nearly 5% within a single day. The blackout of WhatsApp, specifically, which is the most popular messaging service in over 100 countries with over 2 billion active users, caused more anguish for both enterprises and users alike. The blackout also affected several apps that use Facebook login and restricted users to use its much-touted payments service.

Enterprises that use WhatsApp and Facebook Messenger were clueless about the time social media giant will restore its services.

What went wrong?

Facebook attributed the changes in Facebook's server configuration as a reason for the deadlock of its services. It appears that due to the defective configuration changes, the network and backbone routers that coordinate network traffic between Facebook's data centers could not identify the location of their data centers. Many technology experts were quick to suggest that the problem was associated with the Border Gateway Protocol (BGP) route that comprises the IP addresses of its DNA servers.

During the routine maintenance, Facebook explains, these configuration changes caused the DNA servers to go offline. Since the blackout also impacted Facebook's internal systems, even its employees could not collaborate effectively through Facebook Workplace or log in with their work email in many cases.

The event also demonstrated our excessive dependence on a single company to connect and collaborate with colleagues and families in real-time. Facebook's top-notch IT talent's failure to resolve the issue promptly...is a concern

"During one of the routine maintenance jobs, a command was issued to assess the availability of global backbone capacity, which unintentionally took down all the connections in our backbone network, effectively disconnecting Facebook data centers globally. Our systems are designed to audit commands like these to prevent mistakes like this, but a bug in that audit tool prevented it from properly stopping the command," explains Santosh Janardhan, VP - Engineering and Infrastructure, Facebook, in the company's official blog post.

This is akin to the study reflected in the IT Process Institute's Visible Ops Handbook that says that 80% of unplanned outages are caused due to ill-planned changes made by administrators (operations staff or developers).

Santosh adds that the change caused a complete disconnection of Facebook's server connections between its data centers and the internet. And that total loss of connection caused a second issue that made things worse.

Many speculative theories pointed that the services of Facebook were down due to the result of hacking or some malicious activities, a claim that the social media major refuted vehemently. While Facebook mentioned that there was no evidence to suggest the user data was compromised due to the downtime, the company has a history of failing to protect its customers' data, and that's enough to ring the alarm bells in the minds of many users.

Significant impact on enterprises

In recent years, many businesses across the globe have transitioned from email to WhatsApp as the primary instant messaging service to champion two-way communication seamlessly with their customers and employees, replacing erstwhile phone lines and website ways. It has become a preferred medium for a significant population to connect, collaborate and share ideas instantly. There has

As the usage of collaboration tools is growing faster and employees are increasingly sharing documents through these apps, it becomes imperative for organizations who wish to have a greater level of privacy and security, to deploy enterprise-grade messaging apps for enhanced security & business continuity

been an increasing trend where grocery apps, online retailers, and financial institutions reach out to their customers through WhatsApp messages to take timely feedback and verify the delivery of products/services.

WhatsApp Business API has also significantly grown, allowing enterprises to develop more impactful customer engagements through a range of customization. Many in the organizational workforce are also heavily dependent upon WhatsApp groups for real-time internal deliberations and operations management. Many web-goers in India use these social media platforms but do not access the internet, indicating the influence Facebook and WhatsApp hold in the Indian market.

"The disruption was panicking for me as a CEO of a mid-level recruitment firm. For several minutes, I was under the impression that there was a problem with our internet connectivity. When I spoke with my team over a call, I realized that it was a mass outage," says Gaurav Kumar, Managing Partner, G9 Recruiters.

Most small enterprise users did not plan to circumvent such downtime and mitigate the severity of its impact. Even for operational brand-building efforts, they rely heavily on our social media channels. "Our people depend significantly on WhatsApp, Facebook, and LinkedIn to collaborate, generate leads, answer queries, and schedule meetings. During the disruption, we decided to leverage traditional mobile SMS service and emails until the services get restored, but that's not real-time and time taking," echoed Deepak Pandey, Director - Strategy and Technology of Propack Electronics, an Electrostatic Discharge and Clean Room hazard solution provider.

A robust strategy to prevent business paralysis

The outage has again highlighted that despite substantial efforts to strengthen IT infrastructure, enterprises cannot evade downtime incidents and need a robust backup strategy to escape significant losses. On the face of it, using a free app such as WhatsApp for internal or stakeholder communication is certainly not a viable long-term solution for businesses.

As the usage of collaboration tools is growing faster and employees are increasingly sharing documents through these apps, it becomes imperative for organizations who wish to have a greater level of privacy and security, to deploy enterprise-grade messaging apps for enhanced security and business continuity. Such apps also enable organizations to schedule maintenance and updates at a time convenient for them.

Additionally, relatively small companies may not be immediately ready to deploy an alternate messaging strategy but should consider fallback options that can reduce their dependency on a standalone tool and reduce the overall risk in the longer term. For Facebook, too, this could be significant learning and compelled them to revisit their strategy to put their entire DNS servers within their internal network. ■

Facebook's Meta Shakeup Could Help It Thrive In The Enterprise Space

The restructuring will enable Facebook to shift its focus on building future-proof solutions for the hybrid workforce and venture into new technology areas

By Jatinder Singh

Facebook, the world's largest social media company, has rebranded itself as Meta Platforms. With this restructuring, Meta, meaning after or beyond in Greek, has become the umbrella company of Facebook and all former Facebook affiliates, including Instagram, WhatsApp, Messenger, and Oculus VR.

According to Meta, the rationale behind this new identity is to focus on immersive embodied internet, described as the 'metaverse,' by Mark Zuckerberg, the Founder-CEO of Facebook, and now Meta Platforms.

The metaverse narrative essentially revolves around a conceptual idea where internet users can access a shared virtual platform through different devices in real-time to conduct business, collaborate, and play games. Facebook is not the first company to set its ambitions on the metaverse project. Earlier this year, Microsoft too informed that it was building an enterprise metaverse, combining digital and physical worlds in its offerings.

"The next platform will be even more immersive — an embodied internet where you're in the experience, not just looking at it. We call this the metaverse, and it will touch every product we build," Zuckerberg wrote in Founder's Letter, 2021.

Attempt to expand and reinvent

One of the biggest challenges for Facebook had been its etched image of a social media player that it wanted to shift from. With Meta identity, the company aim to be more ambitious and focused on bringing different technology to people. "Right now, our brand is so tightly linked to one product that it can't possibly represent everything we're doing today, let alone in the future. Over time, I hope we are seen as a metaverse company, and I want to anchor our work and our identity on what we're building towards," Zuckerberg mentioned in his blog.

The metaverse narrative essentially revolves around a conceptual idea where internet users can access a shared virtual platform through different devices in real-time to conduct business, collaborate, and play games

Meta's strategy is somewhat akin to what Google did in 2015 by repositioning itself as a wholly-owned subsidiary of Alphabet Inc to reinvest and focus on driverless cars, healthcare technologies, high-speed internet services, devices, among other innovative areas.

With Meta, Zuckerberg seems to aim to expand into domains outside of social media and advertising to become a true technology company and stronger competitor to Amazon and Alphabet.

An umbrella structure enables organizations to be more agile in their approach, achieve growth by aggressive acquisitions and product diversification and improve the overall functioning of distinct identities.

Plummeting reputation, eye on enterprise space

Founded in 2004 by Mark Zuckerberg, the transition is significant for the American online social media giant in two aspects. First, it will allow Meta to reset the brand identity of Facebook, which has been battling with a tumbling reputation and prolonged outages in the recent past.

The tech behemoth with 3 billion users has been facing scrutiny from regulators and governments around the globe, casting severe doubts on the future of its advertising revenue. By bifurcating Facebook, Meta can avert controversies associated with the American online social media giant and allow each separate unit to deploy a unique approach for growth and execution.

Secondly, the transition could open new doors for Meta, just like Alphabet, to create unique and futuristic offerings targeted at enterprise space while moving away from the traditional baggage of just a social media player.

As users gradually move from traditional social networking to real-time instant collaboration tools such as WhatsApp (owned by Meta), Telegram, and voice assistants, Meta needs new ways to fuel its growth in the long run. And what could be a better time than this when the pandemic-triggered hybrid workspace models are emerging in a big way, empowering employees to work from the location of their choice.

Facebook is currently the chief revenue contributor among all the companies that Meta owns. Revenues from Instagram and WhatsApp have seen a healthy surge but are still minuscule. The social media giant relies on ad sales as the primary source of its income and achieved strong financial performance during the pandemic due to the enforced external movement restrictions. However, things have not been all glowing for Facebook and its founder CEO.

Various studies and reports indicate that Facebook and Instagram social media platforms are already witnessing significant engagement decline across markets due to deteriorating trust in its services among the masses. Meta realizes that it needs to expand its horizons and set up a long-term vision before it gets too late.

By leveraging virtual reality and augmented reality and combining them with AI/ML, the metaverse might bring some innovative concepts to trans-

form modern workplaces. The concept would enable Meta to create new platforms, bringing fiction with reality, helping enterprise workers collaborate through perpetual digital avatars in a virtual office environment. So, in the next few years, the organizational workforce might be brainstorming or whiteboard an idea, hanging out, or just having freewheeling conversations over a cup of coffee from different locations and getting a mixed reality experience.

The aspirational concept may be several years away before it becomes a reality. However, Zuckerberg has already envisioned what the future of the internet looks like. He insists living in the metaverse will feel more natural and vivid, and human beings will be teleported instantly as a hologram to be at the office without a commute, at a concert with friends, or with family in the living room even if they are miles away.

Facebook's interest in VR/AR technology is not entirely new, and the company has been trying to build its VR capability since the time it acquired VR-headset firm Oculus in 2014. In August this year, Facebook launched Workrooms, its flagship collaboration experience platform, in beta, allowing selected people to collaborate, communicate and connect remotely in the same virtual room through VR, irrespective of the physical distance. Workrooms are currently in a testing phase and are likely to be part of its meta-universe.

Along with Workrooms, Meta is also likely to create several tools to enhance the gaming and broadcasting experience.

Opens new prospects in cloud business

The metaverse-aligned transition could allow the Silicon Valley giant to expand its wings in the unchartered but ambitious territory of cloud business. Meta may not have publicized its intention around venturing into the cloud infrastructure business openly. However, enterprise cloud could be a new revenue source that the company might explore in the next few years. Much like Amazon and Microsoft, who earn a substantial part of their revenues from enterprise services, Meta, with its brands holding decades of experience in the internet collaboration space, can develop unique cloud and data analytics offerings.

With a Facebook identity that has been entangled in several controversies over the last few years – from allegedly deploying biased algorithms to not taking adequate measures to safeguard its users' data – moving into a new cloud business wouldn't have been so easy if not impossible. The 'trust' factor is one of the prerequisites of cloud business, and historic references often impact buying decisions in enterprise space.

Meta would possibly look at some more acquisitions before it aims to set its eyes on the competitive cloud space.

Overall, it would be exciting to see if Meta could create a new brand identity among users and help Facebook reinvent itself for bigger things. ■

Are You Ready To Face The Next-Level Cybersecurity Threats?

Three areas that enterprises should focus on while formulating new cybersecurity strategy in the hybrid workspace model

By Jatinder Singh

One of the biggest challenges for organizations today is ensuring they have enough armory to combat cybersecurity threats. Especially since the arrival of the pandemic and rapid digitalization, practicing response time to cyberattacks has become a big concern for technology leaders.

The new innovative technologies have triggered a greater risk of data breaches and hacks. The scale and speed at which the attacks are surfacing are unprecedented and demand organizations to continuously evaluate their risk strategies. Trends reveal that the hybrid workspace models give cybercriminals a fragmented perimeter to expand their attack surface considerably by leveraging cutting-

edge technologies such as artificial intelligence and machine learning.

According to a recent report by Fortinet, as organizations continue to expand their networks with new network edges driven by work-from-anywhere (WFA), remote learning, and new cloud services, the rapid rise in connectivity will present an enormous attack opportunity for cybercriminals who would be exploring broader attack surface in the times to come.

While there is no sure-shot formula to create a perfect cybersecurity strategy to manage newer risks, it should enable businesses to anticipate and combat threats proactively should there be a cybersecurity incident. Let's briefly understand how?

Enhance employee information security awareness

With the concept of work-from-home being adopted at a massive scale by organizations, the new digital workforce may still not be fully savvy with security practices needed to be practiced at their end and to what extent their systems can be compromised. Enterprises need to ensure that their dispersed workforce does not think of cybersecurity as a siloed practice being managed only by the IT teams and should have a thorough understanding of efficient cybersecurity and cyber-hygiene practices.

According to a recent study titled "Beyond Boundaries: The future of cybersecurity in the new world of work commissioned by security firm Tenable, 74% of the organizations said the pandemic-related work procedures such as working from home was the primary cause of at least one attack, and 67% mentioned that these attacks specifically targeted their employees working from home. A significant increase in automated botnet attacks and malware has been witnessed among organizations of all scales.

Various incidents have been observed where employees downloaded a malicious file or a video from an unverified source that put networks and systems at risk. The IT teams should conduct frequent educational and training sessions to inform employees about the correct practices, such as the best ways to recognize phishing scams, set strong passwords, and use separate devices for their personal and office work to secure the enterprise IT infrastructure.

Shift your strategic monitoring approach

The biggest challenge for security and IT teams is to manage IT infrastructure remotely. In the hybrid workspace model, the business continuity planning and security operations center teams may not be fully equipped to collaborate effectively and detect threats timely. In his blog, similar sentiments have been echoed by David Ferbrache, Global Head of Cyber Futures KPMG in the UK. "Threat groups are exploiting the enormous workload on IT and security teams and are launching enterprise-level ransomware attacks, crypto-mining operations, and denial of service attacks. Security operations center (SOC) and disaster recovery teams may not be used to, or able to, work remotely or with only a few members on-site at a given time. Now more than ever, detection and rapid response to cyber threats matter," he explains.

Organizations should deploy solutions that offer a more granular approach to network access and authentication... In addition, selecting third-party software vendors and keeping a solid check on them is important

This requires a strategic shift in the overall cybersecurity monitoring approach adopted by organizations. Traditional monitoring capabilities needed to be replaced with new-age practices. Ferbrache suggests that enterprises need to ensure adequate staff and are well-practiced in managing attacks while working remotely. "If staff need to come into work and might be questioned by authorities for doing so, provide them with a letter of authority confirming their importance to your organization," he adds.

Upgrade risk assessment capabilities

Organizations should deploy solutions that offer a more granular approach to network access and authentication in the age of exploding data volumes. In addition, selecting third-party software vendors and keeping a solid check on them is equally important. Recent attacks such as the SolarWinds software supply chain attack are a prime example of how hackers can secretly break into commercial software applications and launch a series of cyberattacks through malicious codes.

Enterprises should look out for well-established options to strengthen their risk and incident response assessment capabilities. Industry experts recommend investments in automation and advanced analytics as a top priority to fortify security practices. Security audits should be more frequent and detailed in the post-pandemic workspace landscape. ■

Double Scoop

Two times the revelation

Souveek Ray

Senior Product Manager, NIKE

MY FAVORITE SOCIAL MEDIA TOOL

LinkedIn

MY FAVORITE POLITICIAN

Arvind Kejriwal

A TECH GURU WHOM I ADMIRE

Vitalik Buterin

A HOLIDAY DESTINATION I'D LIKE TO VISIT TO KICKSTART 2022

London

MY FAVORITE MUSICIAN

Freddie Mercury

MY PEER IN THE IT COMMUNITY

Anirban Mukherjee, Senior Manager - IT, Manipal Health Enterprises

Anirban Mukherjee

Senior Manager - IT, Manipal Health Enterprises

MY FAVORITE SINGER

Hemanta Mukherjee

MY FAVORITE AUTHOR

Sidney Sheldon

WORK FROM HOME OR WORK FROM OFFICE?

Work From Office

A GADGET WHICH I USE THE MOST

Smartphone

MY FAVORITE CAR

Honda City

डिजिट
अब हिंदी में

देश का सबसे लोकप्रिय और विश्वसनीय टेक्नोलॉजी वेबसाइट डिजिट अब हिंदी में उपलब्ध हैं। नयी हिंदी वेबसाइट आपको टेक्नोलॉजी से जुड़े हर छोटी बड़ी घटनाओ से अवगत रखेगी। साथ में नए हिंदी वेबसाइट पर आपको डिजिट टेस्ट लैब से विस्तृत गैजेट रिव्यु से लेकर टेक सुझाव मिलेंगे। डिजिट जल्द ही और भी अन्य भारतीय भाषाओ में उपलब्ध होगा।

digit.in
NOW IN HINDI

www.digit.in/hi
www.facebook.com/digithindi

डिजिट

To follow the latest in tech,
follow us on...

facebook.com/digitgeek

digit.in/facebook

डिजिट
अब हिंदी में

देश का सबसे लोकप्रिय और विश्वसनीय टेक्नोलॉजी वेबसाइट डिजिट अब हिंदी में उपलब्ध हैं। नयी हिंदी वेबसाइट आपको टेक्नोलॉजी से जुड़े हर छोटी बड़ी घटनाओ से अवगत रखेगी। साथ में नए हिंदी वेबसाइट पर आपको डिजिट टेस्ट लैब से विस्तृत गैजेट रिव्यु से लेकर टेक सुझाव मिलेंगे। डिजिट जल्द ही और भी अन्य भारतीय भाषाओ में उपलब्ध होगा।

digit.in
NOW IN HINDI

www.digit.in/hi
www.facebook.com/digithindi

डिजिट

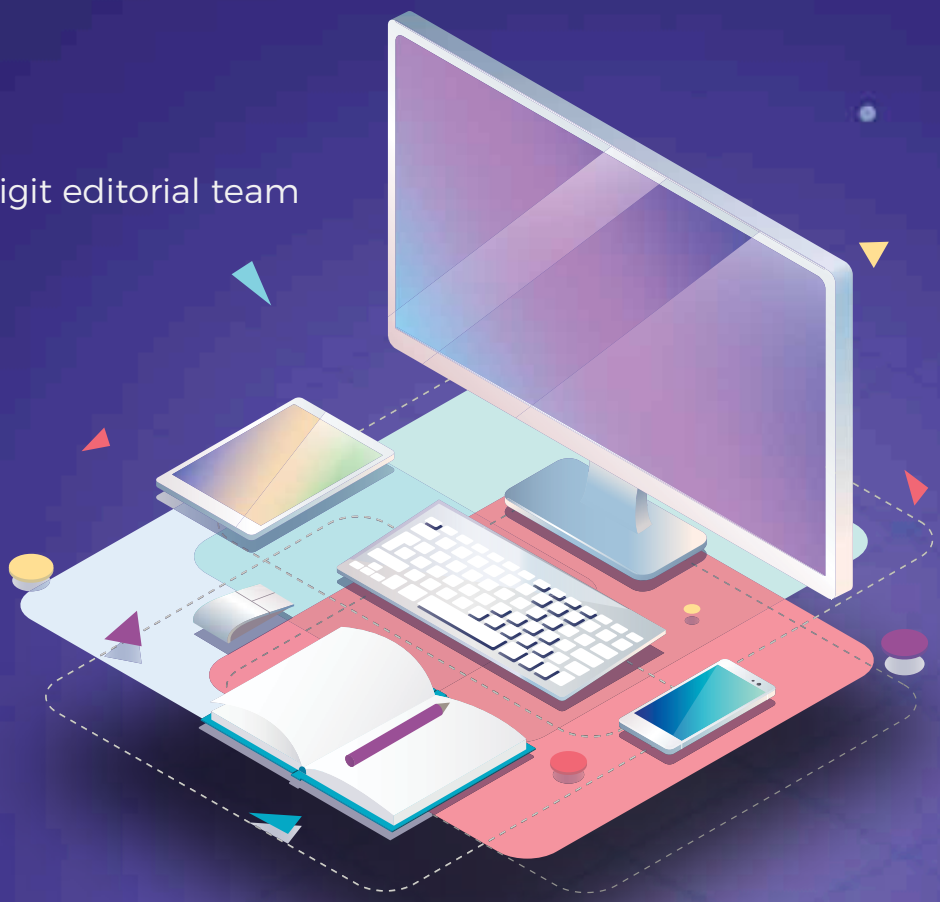
LAUNCHING

digit SQUAD

Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member

- Launch your own tech channel on Digit.in
- Become a Digit Certified tech influencer
- Engage with digit editorial team
- Make money



Apply now by scanning the QR code

www.digit.in/digit-squad/apply.html