






## Gear up for a Digital Workspace

Remote working is an increasing fact of businesses today. While the shift to distributed and remote work has its advantages, it introduces several challenges for business. These include keeping employees productive with secure access to corporate resources.

To perform at their best, employees want access to their data and applications remotely across any number of devices. So, to establish this engagement, IT teams must be able to quickly scale infrastructure and allow instant access to mission-critical apps and data, without compromising security and user experience.

Our whitepaper provides well-research viewpoints on using a modern solution approach for deploying virtual desktops and applications to enable your distributed workforce drive business growth with better-than-before pandemic productivity levels.

### Download the whitepaper to gain insight into:

-  Industry-wise use cases for VDI and apps
-  IT requirements and typical challenges
-  VMware-validated solution for the digital workspace
-  Business benefits
-  Modular deployment options

<https://bit.ly/3vXPoVP>



**Anoop Pai Dhungat**  
Chairman & MD

**MD** SPEAKS

Dear Readers,

*The current wave of COVID-19 that is hitting India is perhaps the worst that the world has seen. The impact on a lot of us has been harsh and direct. Many of us at Galaxy have lost close ones and many others have had close ones in critical conditions. I am sure the same is the case with many of our other stakeholders and readers. My heart goes out to all of you and prayers for the departed to rest in peace and for this scourge to go away as soon as possible so that all of us are safe. This disease is highly contagious and the moment we let our guard down, it strikes. Those who can get vaccinated must get the vaccine and in any case maintain all precautions to avoid getting infected. Masks, hand hygiene and social distancing are a must.*

*We at Galaxy can help you gear up for a digital workspace so that lockdowns don't impact your operations. We offer productivity tools that keep employees productive with secure access to corporate resources. These tools allow users to access their data and applications remotely across any number of devices. Our cloud based solutions enable IT teams to quickly scale infrastructure and allow instant access to mission-critical apps and data, without compromising security and user experience.*

*Please reach out us to see how we can help you in these difficult times.*

*Happy reading*





# Future Is Now

## Scientists train a computer to learn like a human

In a now-famous experiment, Russian physiologist Ivan Pavlov taught his dog to associate food with the sound of a bell ringing, so much so that the dog would start to drool when it heard the sound. This was a demonstration of 'associative learning': how our experiences and memories can lead to unrelated ideas being linked in our brains over time.

Now, a team of researchers at Northwestern University and the University of Hong Kong have developed a device that can learn over time in the same way, mimicking a human brain. This technology could be more energy-efficient than traditional computers, the scientists say, and can even continue to run smoothly when some components fail.

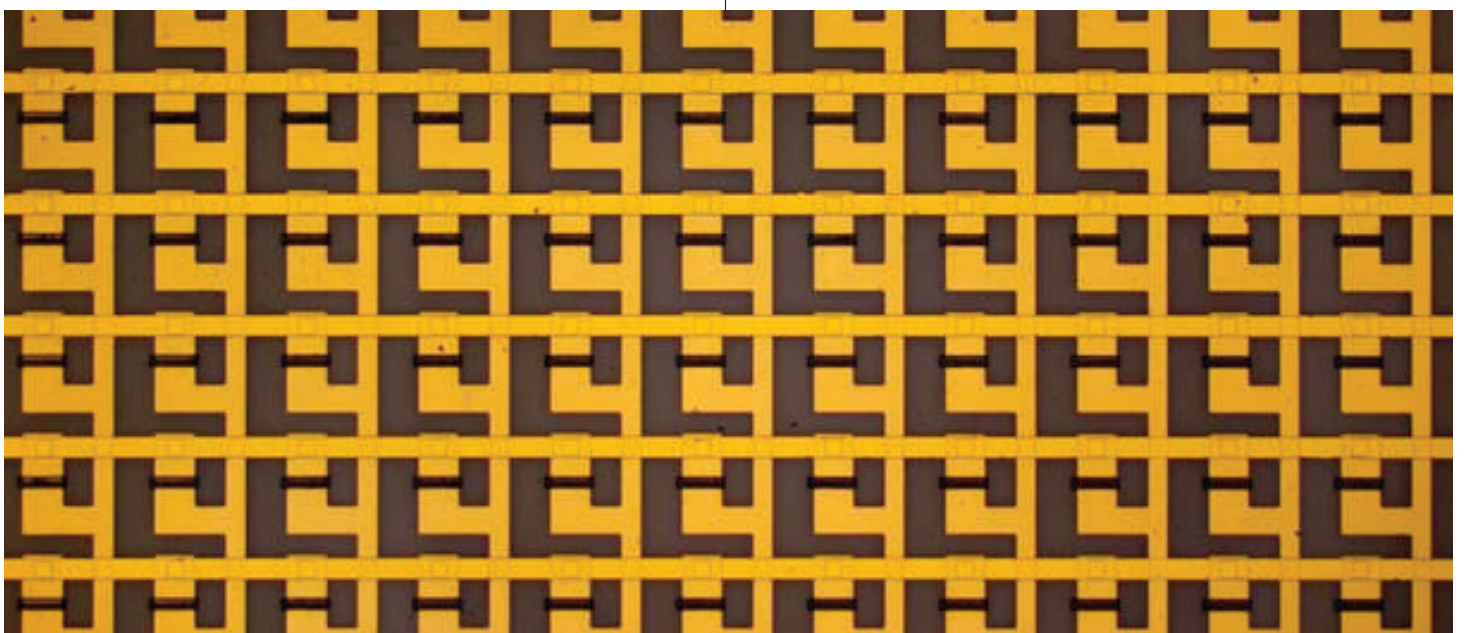
The brain has synapses which connect neurons together and pass messages between them using chemicals called neurotransmitters. Strengthening the connection between two neurons results in the creation of memory.

Inspired by this process, the team developed the 'synaptic transistor', an organic, electrochemical device

that can trap ions. The ions behave like neurotransmitters and trapping them allows the transistor to 'remember' previous activity. This process allows the device to form connections over time. The team conditioned the device to associate light with pressure. First, they pulsed an LED light bulb, which the device picked up with its light sensors, and they immediately followed that by applying pressure to its pressure sensors. After several training cycles, the circuit had formed a significant association between light and pressure. It started to produce a signal corresponding with pressure after only a flash of light.

"Although the modern computer is outstanding, the human brain can easily outperform it in some complex and unstructured tasks, such as pattern recognition, motor control and multisensory integration," said Dr Jonathan Rivnay, Assistant Professor of Biomedical Engineering at Northwestern University and a senior author of the study.

"This is thanks to the plasticity of the synapse, which is the basic building block of the brain's computational power. These synapses enable the brain to work in a highly parallel, fault tolerant and energy-efficient manner."



An array of synaptic transistors © Northwestern University



## Technology Focus

### Gartner forecasts India public cloud end-user spending to total US\$ 4.4 billion in 2021

End user spending on public cloud services in India will total US\$ 4.4 billion in 2021, according to the latest forecast from Gartner. As compared to 2020, end user spending on public cloud will grow 31.4 per cent in 2021.

“Indian CIOs saw the benefits of cloud during the first wave of the pandemic in 2020. To build business resilience and minimise the impact of continued disruptions, investing in cloud is unavoidable. India has experienced consistent double-digit growth in cloud spending over the last three years, the pandemic only expedited the shift,” said Sid Nag, Research Vice President, Gartner.

The continued trend of increased remote workers in 2021 will lead to an increase in spending on desktop-as-a-service (DaaS) and infrastructure-as-a-service (IaaS). These segments are forecast to grow 47.7 per cent and 52.2 per cent, respectively.

For the first time, spending on SaaS and cloud management and security services will experience double digit growth in India. “SaaS has been pivotal in supporting the sudden increase in the mobile

workforce, as well as customers, in 2020. Learning from this, Indian CIOs will continue to build on the above trend as they move towards a composable business environment,” added Nag.

Within SaaS, customer experience and relationship management and content services will be the highest growing segments in 2021, forecast to grow 24.9 per cent and 26.1 per cent respectively. In 2020, spending on e-mail and authoring declined 0.2 per cent, however, this trend will reverse in 2021. E-mail and authoring is expected to grow 25.1 per cent this year. With the increase in remote workers by organisations due to the pandemic, more business is being conducted using email and collaboration tools, which will drive the growth of these services.



<https://bit.ly/3b3rTmi>

### Securing BYO Devices in the Times of Pandemic

Think 2020, think the year that the world changed, and how. To sail the seas of globally imposed lockdowns, gravitating to remote working was the next obvious step that organizations needed to take, no matter what their traditional means of operations were. Conventional organizations that were otherwise hesitant to allow their employees to work from home a couple of days a week or less, had to adopt the new normal if they wanted to keep the business afloat.

#### BYOD Adoption: The Move

With the pandemic ushering in a sudden need for social distancing and isolation, the move to remote work, especially full-fledged, was sudden for most organizations. While some organizations quickly provisioned corporate-owned devices to be shipped to

the employees' location, many resorted to relying on employees' personal devices for a make-shift workstation. The lack of proper compartmentalization of work and personal data on these devices naturally is the biggest threat to corporate data security. Not to mention that if these devices are shared by the employees with others, the risk is higher.

And it is not just about the actual devices used as a part of BYOD. The shared networks these devices are connected to or external peripherals such as printers are also a gateway for attackers.

When employees are working from home full time, it is acceptable that they would be using their personal devices during work hours. Unlike traditional office perimeters where the use of personal smartphones and other connected devices could be restricted, the work from home model automatically brings in the question of devices that employees use while working, not necessarily for work.

While the line between personal and business devices has always been hazy, the pandemic served as the ultimate blow. No longer can organizations control which devices and networks employees are using for work.

As we move forward with a new normal that involves remote working as a near-permanent solution for several jobs and a hybrid work model for several others (once the pandemic dies down, that is), securing BYO devices should be on the ultimate list of priority for organizations and business owners if it already isn't.

### **Here are key steps to bolster BYOD security:**

#### **Have a strong BYOD policy**

This is an organizational activity that needs to be taken up on high priority. Create very specific guidelines on the acceptable usage of devices:

- Enforce a strong password policy for the work apps
- Prevent data copying and sharing from work apps to personal and vice-a-versa
- Ask the employees to disclose the devices that will be used for remote working
- Carry out integrity tests to check if the devices are robust and compatible enough to handle corporate usage and security requirements.
- Ensure the devices are secured with anti-virus software and the corporate data is protected with a firewall
- Make sure that the IT teams have control, such as selective remote wipe over the work containers/apps on the BYO devices.

#### **Manage remote access**

To limit the cyber security risks and the exposure of corporate data to threats, controlling remote access to corporate resources is crucial. Having a re-look at the access permissions, identifying loopholes and revoking privileged access wherever unnecessary is important. However, it should not hinder employee productivity and creating a responsive system to grant access for valid reasons to authorized employees, whenever requested, is critical.

#### **Don't ignore the network security**

Network security can be often overlooked and can prove to be an expensive mistake. When employees are working remotely and are using personal devices, IT can no longer control which networks they are connected to. Routing the traffic to corporate resources and apps via a trusted VPN can help in maintaining network security.

#### **It's not only about the devices**

Sightline and eavesdropping are modern security

concerns that are on the rise, thanks to the hyper-connected homes with smart home assistants and virtual assistants. While sightline can be mitigated by gesture or biometric-based access, eavesdropping and lurking by several other devices present within the home office can be a major security loophole.

Employee education and awareness are hence critical, employees need to be trained extensively on impending security threats and the measures that need to be taken on their end- something as simple as not sharing passwords, not opening malicious emails that pretend to be COVID-19 related information, switching off other devices while working or taking work calls and confidential meetings from a room free of virtual assistants.

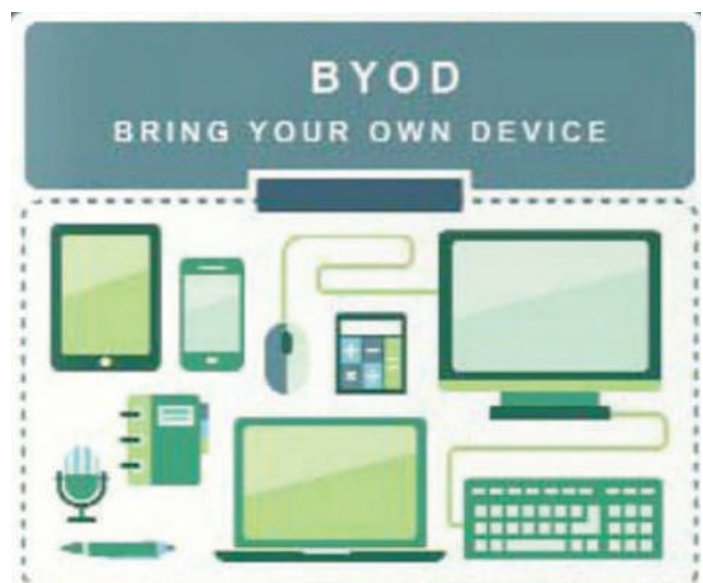
Remember, your organization's security posture is only as strong as your employees want it to be!

#### **Remote implementation is essential**

The policy implementation and enforcement, especially during the pandemic, needs to be quick and remote. The IT teams can not physically enroll the devices used by their employees and hence the implementation needs to be fully remote, with minimum end-user intervention. Since the IT teams are in for a long stretch due to fully remote working, the monitoring and management of BYO devices also need to be fully virtual and effortless.

Hence, investing in the right Mobile Device Management system is emphasized, which can help with policy enforcement, management and monitoring for a fragmented BYO device inventory.

Implementing BYOD is no piece of cake, especially when the organization has a large, dispersed workforce. But with the right approach and the right set of tools, it can be streamlined, not just for the pandemic but beyond.



<https://bit.ly/3xLLDo3>



# Special Focus

## F5 Local Traffic Manager

F5 big ip devices work on a modular system, so you can add new functions—as necessary—to quickly adapt to changing application and business needs. F5 BIG-IP Local Traffic Manager (LTM) helps you deliver your applications to users in a reliable, secure, and optimized way. By making intelligent traffic decisions that adapt to the changing demands of your applications, BIG-IP LTM ensures their consistent availability and scalability. With BIG-IP LTM, you have the power to simplify, automate, and customize applications faster and more predictably. The following modules are available for the BIG-IP system, including BIG-IP LTM.

### Key benefits

- Deliver applications rapidly and reliably.
- Automate and customize with programmable infrastructure.
- Transition to SDN and cloud networks.
- Easily deploy and manage applications.
- Secure your critical applications

### BIG-IP DNS

F5 BIG-IP DNS distributes DNS and user application requests based on business policies, data center and network conditions, user location, and application performance. BIG-IP DNS delivers F5's high-performance DNS services with visibility, reporting, and analysis; scales and secures DNS responses geographically to survive DDoS attacks;

delivers a complete, real-time DNSSEC solution; and ensures global application high availability.

### Key benefits

- Scales DNS to more than 10 million RPS with a fully loaded chassis.
- Gains control and secures global application delivery.
- Improves application performance.
- Deploys flexibly, scales as you grow, and manages your network efficiently.

### BIG-IP Application Security Manager

F5 BIG-IP Application Security Manager (ASM), built on proven F5 Advanced WAF technology, redefines application security and addresses the most prevalent threats organizations face today. It proactively detects and mitigates bots, secures credentials and sensitive data, and defends against application DoS. BIG-IP ASM is offered as an appliance, virtual edition, and as a managed service .

### Key benefits

- Protects against malicious bots.
- Safeguards credentials and sensitive data.
- Defends against sophisticated application DoS.
- Ensures application security and compliance.

**For a free consultation, please contact us on 022-46108777 or email us at [marketing@goapl.com](mailto:marketing@goapl.com)**





## Google and Vodafone are building a powerful new data platform

Google and Vodafone announced they're extending their partnership by six years, in part to build a powerful new data platform that can support the movement of 5,000 data feeds per day to the cloud.

The platform will allow Vodafone to better leverage its vast sums of data, so they can offer new digital products and services to customers globally. While Vodafone and Google are building the platform to serve the telecom giant's needs, the companies will also explore the possibility of providing consultancy services to other businesses, either jointly or independently.

Vodafone first decided to move its large, on-premise big data systems to the Google Cloud Platform (GCP) more than two years ago. Now, as part of their extended partnership, Vodafone is re-platforming its SAP system and moving them to GCP.

They're also co-innovating the new platform, called Nucleus, to integrate all of Vodafone's global data with a standard data model and common processes, data sourcing and data products. The platform critically relies on clear lineage and strong data governance capabilities from Google Cloud.

The Nucleus platform will house a new system called Dynamo, which will extract and manage data from source systems and distribute it in a standard format. The system can support the equivalent of 50 terabytes of data per day. The system should avoid redundant data extraction efforts, thanks to reusable connectors and data pipelines. And by basing all the user interfaces on common APIs and strong security and compliance protocols, it should encourage the re-use of data and compliance with data standards across markets.



<https://zd.net/33fv0mS>

## India's edtech industry to become US\$ 30 billion industry by 2032.

India's edtech sector to become a US\$ 30 billion industry in the next 10 years on the backing of growing demand and strengthening business models, according to RBSA Advisor, a transaction advisory firm specialising in valuation, investment banking and transaction services.

Vigorous growth will drive the growth in the K-12 edtech opportunity in user base, with edtech users growing proportionately faster than the overall student base. Online education offerings for Classes 1st to 12th are projected to increase 6.3X by 2022 from the base of 2019, creating a US\$ 1.7 billion market, while the post-K12 market will grow 3.7X to touch US\$ 1.8 billion.

The New Education Policy 2020 offers multiple exit options and certification within the undergraduate education period and an academic bank of credit will be established for digitally storing academic credits earned from different institutes so that these can be transferred and counted towards the final degree earned.

India has emerged to be among the top three countries in the world after China and the USA to get venture capital funding in the edtech sector. Global edtech started the last decade with US\$ 500 million of venture capital invested in 2010 and finished 32x higher at US\$ 16.1 billion in 2020, nearly 2x the previous investment record in 2018.

The US and China continue to grow, along with the spectacular rise of India as an edtech powerhouse. India's edutech sector has attracted private equity investments of around US\$ 4 billion in the last five years which has led to the emergence of global edtech leaders like Byju's commanding a valuation of US\$ 15 billion.

"Lockdown because of the pandemic has resulted in a massive increase in the private equity investments in the edtech sector because of increasing inclination of students and parents to opt for getting an education from home through various learning platforms," Rajeev R. Shah, Managing Director and CEO, RBSA Advisors.

<https://bit.ly/3h5C11r>

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