@entitworld @enterpriseitworld @enterpriseitworld

RS 20 | PAGES 42 | VOLUME 08 | ISSUE 12 WWW.ENTERPRISEITWORLD.COM

Enterprise IT WORLD

FOR THE CIOs. BY THE CIOs.

MARCH 2024

Enterprise IT WORLD
FOR THE CIOs, BY THE CIOs

CIO ACCELERATOR X AWARDS 2024

5 CITIES EVENT

CHENNAI	DELHI	MUMBAI	BANGALORE	KOLKATA
				
17 MAY 2024	7 JUNE 2024	21 JUNE 2024	5 JULY 2024	19 JULY 2024

WWW.CIO500.IN

FOLLOW US ON

/Enterpriseitworldmea /EntITworldmea /CIOTV / CEOTV /Enterpriseitworldmea

CONTACT US

6/102, Kaushalya Park, Hauz Khas New Delhi-110016
Phone: 91-11-40587445 E-mail: info@accentinfomedia.com

ARE WE READY FOR NEXT FIVE YEARS TEC EVOLUTION **IN INDIA?**

Hello Friends.

As we are moving closer to the end of FY 23, there is an uncertainly and unknown restlessness coming into everyone's mind that the year ends and we are entering into a new FY what is unfolding? For sure, the first big event in our life is the Parliament Election 2024 from April to June and followed by the new government formation. Depending on the new government there would be new agenda and new mandate also for the public. But what about us as stake holders of technology? Will there be any change in the mandate of the new government from policy point of view? I think first the incumbent government is going to rein for the consecutive 3rd term. There would be more speed in implementation of digitization in government level with better and favourable policy for the country.

My argument is very simple that the party in the centre is nationalist. It takes pride in creating name of India in the global community and other advanced countries. The decision makers take pride in taking make-in-India products and services to global market. This government or this party understands the lacune within the system. The government also understands the potential of the country along with the distinct advantage vi-s-vis rest of the word in the race of becoming powerful businesswise.

So, for next 5 years, if the political situation remains good, which all hope to, one can see a lot of tech innovation coming of India. We can see global investors' mood swing has happened in favour of India. Gradually there is a shift in investment destination in the world in every sector – led by manufacturing in railway sector, defence sector, energy sector, etc. The global investors now realise that there is better ROI in India than other countries.

So, the overall impact to the IT ecosystem is growth. There would be multiple JVs & M&A, there would be multiple offshoots, there would be multiple new companies and startups in the industry. Yesterday I saw a report which puts Gurgaon on the startup ecosystem growth score at 15, whereas Dubai is no.1. So, the government is watching the activities and definitely thinking of improving on this score.

India has already its own GDPR policy in the form of DPDP (Digital Personal Data Protection At), it would pave way to setup a big number of Datacentres. The government has also its own AI policy. So, in total, the next 5 years would see a lot of churning in the industry and there is going to be a lot of action in the country from the IT perspective. Every state wants to attract investment into their states … have their own agenda which is different from that of the centre.

Look what is happening in the election! The entire country and its future certainly hangs on a balance.

In the meantime, we at Enterprise IT World want to connect and network with CIOs and IT Heads across 10 cities. In the first phase, we would connect five big city CIOs including Delhi, Mumbai, Bangalore, Chennai and Kolkata and in the second phase would connect with another five cities – most preferably Tier- 2 Cities.

SANJAY MOHAPATRA
SANJAY@ACCENTINFOMEDIA.COM

NEXT MONTH SPECIAL

COVER STORY

FUTURE OF DATA CENTRE

The next issue is dedicated to the Future of Data Centre We would like to take feedback from the CIOs and OEMs and create our judgment on the same.

SUPPLEMENT

QUOTES FROM TOP CIOS

The supplement story of the magazine would have relevant quotes from the top CIOs in India.

PLUS

Interviews and Case Studies

Catch interviews, guest articles and case studies of recent applications from the Industry stakeholders, IT/ITES Vendors and IT leaders and CIOs from the Enterprise IT World CIO Community.

Send in your inputs to sanjay@accentinfomedia.com

CONTENTS

VOLUME 08 | ISSUE 12 | MARCH 2024 | WWW.ENTERPRISEITWORLD.COM

SOPHOS

MORE INSIDE

Enterprise IT WORLD
FOR THE CIOs. BY THE CIOs

Publisher: Sanjib Mohapatra
Chief Editor: Sanjay Mohapatra
Associate Editor: Balaka Baruah Agarwal
Managing Editor: Anisha Nayar Dhawan
Designer : Deepak kumar
Web Designer: Sangeet Kumar
Technical Writer: Manas Ranjan
Lead Visualizer: DPR Choudhary

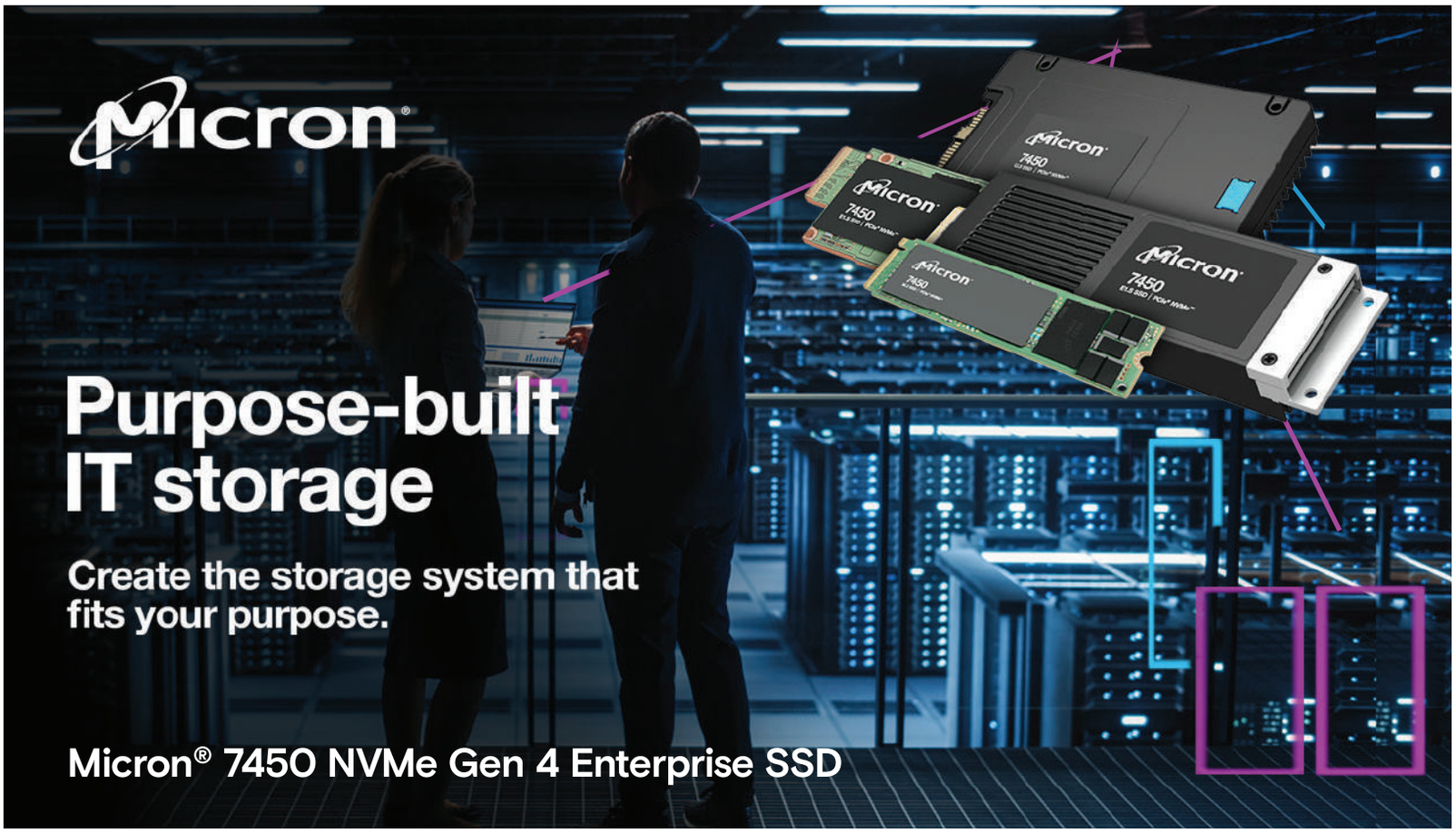
MARKETING
Marketing Manager: Lagan Sehgal

SALES CONTACTS
Delhi 6/102, Kaushalya Park, Hauz Khas
New Delhi-110016
Phone: 91-11-40587445
E-mail: info@accentinfomedia.com

EDITORIAL OFFICE
Delhi: 6/103, (GF) Kaushalya Park, Hauz Khas
New Delhi-110016,
Phone: 91-40587445
info@accentinfomedia.com

Printed, Published and Owned by Sanjib Mohapatra
Place of Publication: 6/103, (GF) Kaushalya Park, Hauz Khas
New Delhi-110016
Phone: 91-11-46151993 / 41055458
Printed at Karan Printers, F-29/2, 1st floor, Okhla Industrial Area, Phase-2, New Delhi 110020, India.

Subscription: Rs.200 (12 issues)
All payments favouring: Accent Info Media Pvt. Ltd.



Best for

- Hyperconverged infrastructure
- Cloud infrastructure Big data
- Object storage

Sequential Reads
Up to 6800MB/s

Sequential Writes
Up to 5600MB/s

Capacity
Up to 15.36 TB

Warranty
5-year limited

Key Features

- Power loss protection
- Enterprise data path protection
- Firmware activated without reset
- Secure erase & Secure boot

Contact Us - Expert Talk

Mr. Sanjeeo Singh: VAR/SI Channel Manager
Contact: +918800507776

ITWORLD ROUND UP

NetApp Turbocharges AI Innovation with Intelligent Data Infrastructure

NetApp introduces enhanced features to boost the effectiveness of generative artificial intelligence (Gen AI) endeavors, empowering users to gain a competitive edge. By integrating NetApp's smart data infrastructure with NVIDIA's high-performance compute, networking, and software, customers can elevate their AI initiatives.

Gen AI has captured global attention for its potential to automate tedious tasks, uncover new insights, and drive product innovation. Nearly three out of four companies are already using Gen AI, according to the NetApp 2023 Data Complexity report. To unlock the potential of Gen AI, organisations need secure, high-performance access to data spread across complex hybrid and multicloud environments. NetApp has a long and successful history of expertise in supporting AI with solutions that deliver management simplicity anywhere data lives, provide high performance without requiring new infrastructure silos, and supply trusted, secure data to drive responsible AI.

"NetApp is the intelligent data infrastructure company, with solutions optimised to unleash the full potential of our customers' investments in AI", said Ravi Chhabria, Managing Director at NetApp India. "Our distinct approach to AI provides complete access and control over their data across the entire pipeline, moving seamlessly between public cloud and on-prem environments."

DATA BRIEF

According to International Data Corporation (IDC), IT spending in India for 2024 is expected to grow 11% year-on-year (YoY), reaching USD $44 billion in 2024.*

Source: Gartner

CoforgeLaunchesOrion:AI-PoweredSelf-Service for Better Customer Experience

Coforge Limited introduces Coforge Orion, a Gen AI-based self-service solution automating customer interactions through generative AI. It handles outbound and inbound calls, engaging customers, offering intelligent responses, and taking autonomous actions, surpassing traditional automation.

Coforge Orion moves the beyond traditional scripts and messaging based communication and utilizes advanced AI to have natural, personalized conversations with each customer, adapting to the unique flow of each interaction. This empowers businesses in various fields, like travel and healthcare, to automate communication while fostering deeper connections with their customers.

"Coforge Orion is a sophisticated and enterprise grade AI platform built for bi-directional human-like conversations to support sales, marketing and customer service. It can make automated outbound calls to prospects by dynamically generating voice conversations using large language models and can handle inbound inquiries using generative AI capabilities of speech-to-text and text-to-speech" said, Vic Gupta, Executive Vice President, Coforge.

Coforge Orion empowers businesses to deliver exceptional customer experiences and optimize operations by leveraging the power of generative AI. Customers can engage with intelligent virtual agents 24/7, overcoming language barriers with multilingual support, and enjoy seamless interactions through familiar channels like WhatsApp and SMS. Businesses benefit from effortless integration with existing CRM systems and third-party APIs, while autonomous agents address challenges like high error rates and resource-intensive training. Coforge Orion has already helped businesses optimize budgets, strengthen customer satisfaction, and boost revenue through successful pilots. This innovative solution, tailored for industries like travel, banking, insurance, and healthcare, elevates customer interactions and empowers businesses to thrive in today's dynamic landscape.

NETGEAR Launches GS108X and GS108MX 8-Port Gigabit Switches

NETGEAR launches new unmanaged switches, GS108X and GS108MX, for growing businesses and faster device speeds. Both have 8 Gigabit Copper Ports for seamless uplinking. GS108X has a 10Gig SFP+ Port for high-speed connections up to 100 meters, while GS108MX has a flexible 10G/Multi-Gig Port adjusting to speeds from 100M to 10G, including 1G, 2.5G, and 5G increments

Marthesh Nagendra, Sales Director, India MEA South-East Asia Region, NETGEAR said "The launch of our latest switches marks a pivotal moment for businesses seeking sustainable solutions without compromising performance. With a steadfast commitment to energy efficiency and rigorous durability testing, our switches deliver not only cost savings but also the reliability crucial for modern enterprises."

These switches come in a sturdy metal case that can live in a variety of places, including mounted on a wall or under a table. The fanless design also allows the switches to operate silently in a noise-sensitive environment.

CIO EVENTS

16 FEB, 2024
Digital Summit 2024
PLACE: **NEW DELHI**

22 MAR, 2024
BFSI Summit 2024
PLACE: **MUMBAI**

26 APR, 2024
IT / ITES Summit 2024
PLACE: **BANGLORE**

17 MAY, 2024
Manufacturing Summit 2024
PLACE: **CHENNAI**

InstaSafe
Cloud. Secure. Instant.

Gartner

High Performer
WINTER
2022

DSCI
Excellence Awards
2021

~~Latency Issues with VPN~~

Switch to InstaSafe Zero Trust Now!

Onboarding channel partners to capitalize on the fast growing Zero Trust market.

Apply now

sales@instasafe.com

https://instasafe.com

San Francisco | Bangalore | Mumbai | Germany

IBM Transforms Content Creation & Marketing Using Adobe Firefly AI

Last year, while browsing through your social media feeds, you might have been among the hundreds of thousands captivated by a striking image from IBM's "Let's Create" brand campaign, highlighting the company's commitment to co-developing technology solutions with partners.

In the past, it would have taken a company's creative and marketing team days — if not months — to develop assets like these. But this image was part of an early pilot with Adobe Firefly, which put commercially-viable generative AI directly into the IBM teams' workflows. Using simple text prompts, the IBM team was able to generate 200 assets and over 1,000 marketing variations for the campaign in a matter of minutes.

As impressive as these images are, most notable of all, the campaign performed well above IBM's benchmark, driving an impressive 26 times higher engagement, and reaching valuable audiences — 20 percent of respondents were identified as C-level decision makers.

As impressive as these images are, most notable of all, the campaign performed well above IBM's benchmark, driving an impressive 26 times higher engagement, and reaching valuable audiences — 20 percent of respondents were identified as C-level decision makers.

S/HE SAID IT

VIV DA ROS
CIO, CALTEX AUSTRALIA

"To me the organisational culture and structure, including the mindset of the CEO and the board is key to driving positive innovation initiatives and outcomes in business."

"To create a more diverse and inclusive tech world, we need to inspire and empower the next generation of female role models to pursue and develop their career in technology and become innovators, leaders and entrepreneurs."

ANNA RADULOVSKI, FOUNDER & CEO AT WOMENTECH NETWORK

QUICK BYTE ON SECURITY

Rackspace Tech's FAIR: 70% Trained in Gen AI

Rackspace Technology celebrates a major milestone with 70% of its employees, called "Rackers," completing Gen AI training, signaling a significant step forward in the company's strategic growth. This achievement is part of Rackspace Technology's overarching initiative, the Foundry for Generative AI by Rackspace (FAIR™). FAIR™ is a global unit of AI specialists dedicated to accelerating the sustainable adoption of Responsible AI solutions in businesses across various industries.

AddOnNetworksTransceivers:Ideal for AI/ML Apps

AddOn Networks introduces a new lineup of 800G transceivers, facilitating AI, ML, and automation in data center applications. Compatible with InfiniBand and Ethernet, the range provides customers with a compelling alternative to NEMs for building and maintaining advanced optical networks.Data centre operators need extensive data, storage and compute capabilities to ensure the enhanced speeds and low latency required to overcome growing industry demands. AI and ML tools optimise existing infrastructure and establish accurate data analytics for faster decision-making and increased automation. Yet the amount of bandwidth necessary for these to operate successfully, and the lack of compatible solutions in the market, makes selecting the right product a challenge. With this product launch, AddOn Networks will provide operators with the means to optimise their existing networks, alongside a premium support service and a reduction in part lead times.

"This family of transceivers mark an exciting new era for AddOn Networks," said AddOn Networks' Director of Product Line Management Ray Hagen. "Businesses operating in the data centre industry may already be aware of the benefits of 800G transceivers, but when ordering these directly through NEMs, they often experience long lead times and unnecessary delays in delivery. With our new range of transceivers, we will compress the timeline from order to delivery to ensure customers get solutions exactly when they require them. As a result, operators can maximise data centre output through AI and ML tools while making essential cost and time savings."

CloudflareAIFirewall:Securing AIAppsatScale,FreeofCharge

Cloudflare introduces Firewall for AI, offering protection against abuse and attacks targeting Large Language Models (LLMs). Leveraging its expansive global network, Cloudflare aims to safeguard LLM functionality, critical data, and trade secrets from the next wave of AI-based threats.

A recent study revealed that only one in four C-suite level executives have the confidence that their organizations are well-prepared to address AI risks. When it comes to protecting LLMs, it can be extremely challenging to bake in adequate security systems from the start, as it is near impossible to limit user interactions and these models are not predetermined by design – e.g., they may produce a variety of outputs even when given the same input. As a result, LLMs are becoming a defenseless path for threat actors – leaving organizations vulnerable to model tampering, attacks and abuse.

"When new types of applications emerge, new types of threats follow quickly. That's no different for AI-powered applications," said Matthew Prince, Co-Founder & CEO at Cloudflare."
With Cloudflare's Firewall for AI, security teams will be able to protect their LLM applications from the potential vulnerabilities that can be weaponized against AI models.

EXECUTIVE MOVEMENT

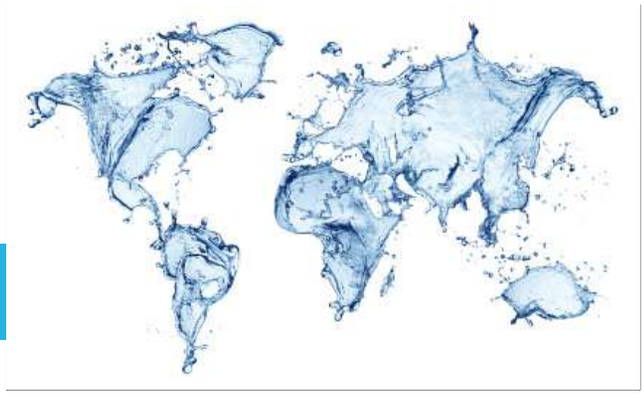
AVEVA Appoints Joanna Mainguy as New Sustainability Accelerator Director

Kunal Ruvala Joins Palo Alto Networks as SVP & GM for India Dev Centers

SG Analytics Welcomes Dr. Das Dasgupta to Its Advisory Board

Brian Pawlowski Joins Hammerspace as VP of PerformanceEngineering

Infopercept Appoints Prashant Pratap Singh as Govt & PSU Sales Director



GLOBAL UPDATE

Pharmarack Transforms Indian Healthcare with Informatica

Informatica's intelligent MDM on AWS is chosen by Pharmarack. This SaaS offering, part of Informatica's AI-powered IDMC, supports Pharmarack's mission to digitize India's pharma ecosystem, enhancing transactions between stockists, chemists, and pharmaceutical companies nationwide.

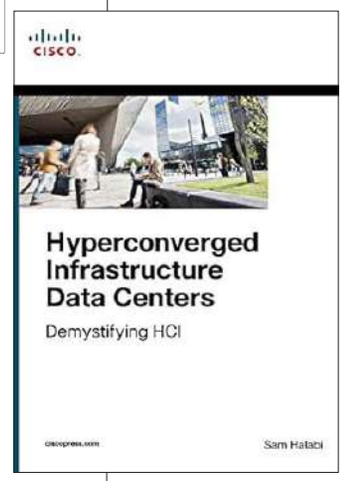
Pharmarack is a pioneering commerce-to-insights technology company addressing core trade challenges encountered by the Indian pharmaceutical industry. Acting as a catalyst, Pharmarack empowers general pharmaceutical trade with a national reach of more than 250,000 chemists and druggists and over 12,000 distributors and stockists trading in more than 300,000 SKUs across six thousand brands. One of the fundamental trade challenges in a marketplace is the consistency of the data catalog throughout the value chain, a problem that Pharmarack aims to resolve using Informatica's intelligent MDM. Arundhati Kshirsagar, Chief Data & Analytics Officer at Pharmarack, said, "Informatica's intelligent MDM enables us to address an industry problem related to catalog quality in both online and offline marketplaces"

Resolving data catalog inconsistency and achieving a single golden record when trying to merge more than 12,000 unique independent catalogs is a significant challenge if done manually. With Informatica's intelligent MDM, Pharmarack aims to tackle this problem for an entire industry offering small and medium businesses in India with catalog quality comparable to that of giant e-commerce players. This solution could be used by more than a million chemists and stockists, enabling them to harness the potential of digital technology without concerns about catalog consistency.

"Informatica is pleased to work with Pharmarack in addressing their catalog challenges by providing our market-leading intelligent MDM solution powered by our metadata AI-driven IDMC platform, to resolve issues related to inconsistent, incomplete and inaccurate data, while enabling a 360-degree view of trusted data for users to perform their tasks more effectively," said Steven Seah, Informatica Managing Director, ASEAN, India, and Korea."

BOOK SHELF

Hyperconverged Infrastructure Data Centers: Demystifying HCI



BY
SAM HALABI

PRICE
RS. 888.00 (PAPERBACK)

WHERE
AMAZON.IN

About The Book

In Hyperconverged Infrastructure Data Centers, best-selling author Sam Halabi demystifies HCI technology, outlines its use cases, and compares solutions from a vendor-neutral perspective. He guides students through evaluation, planning, implementation, and management, helping them decide where HCI makes sense, and how to migrate legacy data centers without disrupting production systems.

About the Author

Sam Halabi is a well-known industry figure with many years of experience in the field of information technology, multicloud, hyperconvergence, enterprise software, and data networking.

P&O Cruises, Cunard Partner with Coforge for Quality Engineering

Coforge Limited and Carnival UK enter a multi-year collaboration to bolster Quality Engineering and Testing capabilities for P&O Cruises and Cunard. The objective is to deliver seamless holidays and exceptional guest experiences amidst the digital era.

The strategic alliance extends beyond QE and Testing, elevating the operational capabilities of the brands. As their sole QA and Testing supplier, Coforge is committed to analysing and optimising every critical system, facilitating a seamless journey through digital transformation.

With expertise in the travel and hospitality industry, Coforge's proven QE and Testing methodologies enable P&O Cruises and Cunard to deliver service excellence across its operations. Automation, data-driven insights, and meticulous testing procedures from Coforge will significantly boost operational efficiency, enhancing performance from shore to sea. Coforge's partnership encompasses all facets across shore, fleet and digital.

This proactive problem-solving approach will enable pre-emptive address of potential issues, maintaining operational smoothness and the traditionally high thresholds of guest satisfaction. This strategy and improved resources bolster reliability and efficiency, supporting digital transformation ambitions.

By prioritising comprehensive testing, P&O Cruises and Cunard aim to provide exceptional guest experiences, surpassing expectations at every touchpoint. This holistic strategy, driven by Coforge's Centre of Excellence (COE) in QE & Automation envisions a future of outstanding experiences, reinforcing the industry leadership of both brands.

Akamai Enhances App & API Protector with New Security Features

Akamai Technologies enhances its App & API Protector with advanced defenses against complex application-layer DDoS attacks. The upgraded Layer 7 protections effectively identify and counter short attack bursts and utilize client reputation scores for better rate limiting. App & API Protector also now features Browser Impersonation Detection, which uses machine learning to gain deeper insights into browser behaviours while minimising false positives and enabling more effective detection of malicious bots.

"The evolution of Akamai App & API Protector highlights our focus on innovation and a customer-centric approach," said Rupesh Chokshi, Senior Vice President and General Manager of Application Security at Akamai. "

"We love working with Akamai. They consistently deliver great reliability and performance through their solutions, which are also fully compliant with the latest security regulation," said Jerome Etienne, Group Chief Information Security Officer at Groupe Rocher."

CriminalsExpandCryptocurrencyFraudGloballywith Sha Zhu Pan Kits

Sophos uncovered a new cybercrime trend: "sha zhu pan" scammers are selling kits on the dark web, expanding globally. These kits, used for cryptocurrency fraud, originate from China and facilitate schemes like "DeFi savings."

Criminals position DeFi savings scams as passive investment opportunities that are similar to money market accounts, often times to people who have no understanding of crypto. Victims only need to connect their crypto wallet to a "brokerage account," with the expectation that they will earn significant interest from their investment. In reality, victims are adding their crypto wallets to a fraudulent cryptocurrency trading pool, which the fraudsters then empty.

"As with other types of commercialized cybercrime, these kits lower the entry barriers for cybercriminals interested in pig butchering and vastly expand the victim pool. Last year, pig butchering was already a multi-billion-dollar fraud phenomenon; sadly, the problem is likely only to grow exponentially this year," said Sean Gallagher, principal threat researcher, Sophos.

Cohesity Unveils First AI Search Assistant for Data Transformation

Cohesity unveiled Gaia, an AI-powered enterprise search assistant, integrating RAG AI and LLMs to analyze backup data in Cohesity setups. Gaia, available March 15, lets users ask questions and get answers from their enterprise data.

The underlying architecture of Cohesity Data Cloud manages and secures data with a unique blend of performance, extensibility, and scale. Cohesity Gaia extends the value proposition of Cohesity Data Cloud even further:

By building a RAG AI solution on Cohesity's multicloud platform, Cohesity will be able to seamlessly provide RAG AI conversational search experiences across cloud and hybrid environments that will allow enterprises to gain deeper insights into their data and make informed decisions in the future, no matter where their stored data resides.

"Enterprises are excited to harness the power of generative AI but have faced several challenges gaining insights into secondary data, including backup, archived and vaulted data – because every approach requires re-hydrating the data, and painfully waiting weeks for the data to be available for analytics and insights. Cohesity Gaia dramatically simplifies this process with our patent-pending approach using Retrieval Augmented Generation," said Sanjay Poonen, CEO and President, Cohesity."

DIGEST

ORACLE AIDS FIRMS IN ATTAINING PEAK SCALABILITY,AVAILABILITY,ANDMEETING DATA SOVEREIGNTY DEMANDS

Oracle unveils Oracle Globally Distributed Autonomous Database, leveraging sharding tech for data control and distribution. It empowers organizations to automatically spread data worldwide, ensuring scalability, availability, and sovereignty compliance. This autonomous solution slashes costs while enhancing operational efficiency.

As a full-featured, converged database, Globally Distributed Autonomous Database simplifies the development and use of distributed databases for mission-critical applications by supporting virtually any data type, workload, and programming style at scale.

UIPATH & GOOGLE CLOUD EXPAND PARTNERSHIP TO BOOST GEN AI

UiPath announced an expanded partnership to extend customers' ability to transform their enterprise with AI-powered automation. UiPath, a Premier Level partner of Google Cloud, is now available on Google Cloud Marketplace, making it easier for Google Cloud customers to purchase the industry leading UiPath Business Automation Platform and reliably deploy and scale their automation initiatives on Google Cloud infrastructure. UiPath is expanding its partnership with Google Cloud to help customers facilitate their AI-powered automation journey while integrating with Google Cloud's Vertex AI and Google Workspace business collaboration offerings.

KEEPER SECURITY JOINS THE AWS PARTNER NETWORK

Keeper Security has partnered with Amazon Web Services (AWS), joining the global network of 130,000 partners from over 200 countries. This move aims to meet the increasing need for strong account security amidst rising cyber threats, bolstering digital protections for businesses worldwide.

"AWS has long been recognised as the leading cloud services provider and we're proud to meet their rigid standards and bring their technical advantages to public and private-sector business and enterprise customers," said, Darren Guccione, CEO and Co-founder, Keeper Security."

Keeper provides a full suite of award-winning consumer and business offerings in password, secrets and privileged connection management, as well as differentiators that set Keeper apart from its competitors.

MANAGEMENT **MANTRA**

"Most d is happening within the smaller organisations with specialist capabilities."

Mike Wright, CIO, McKinsey & Company

H.M King Charles III confers Honorary Knighthood (KBE) on Sunil Bharti Mittal for advancing India – UK business relations

Sunil Bharti Mittal has become the first Indian citizen to be awarded Honorary Knighthood, the Knight Commander of the Most Excellent Order of the British Empire (KBE), by King Charles III.

The KBE is among the highest honours conferred by the British Sovereign to civilians. It is awarded in an honorary capacity to foreign nationals.

Sunil Bharti Mittal said, "I am deeply humbled by this gracious recognition from His Majesty, King Charles. UK and India have historical relations, which are now entering a new era of increased cooperation and collaboration"

He added, "I remain committed to working towards strengthening the economic and bilateral trade relationships between our two great nations. I am thankful to the Government of UK, whose support and keen attention to the needs of business has been critical in making the country an attractive investment destination."

In 2007, Sunil was bestowed with the Padma Bhushan, one of India's highest civilian honours, awarded to individuals for demonstrating distinguished services of high order.

Bharti in the UK

Bharti's Airtel Africa was successfully listed on the London Stock Exchange in 2019, and is a constituent of the FTSE100 Index.

Sunil successfully led the revival of OneWeb (now Eutelsat), leading a consortium with the UK Government and other strategic investors to offer satellite broadband services globally.

Neo4j Collaborates with Microsoft to Advance GenAI and Data Solutions

Neo4j collaborates with Microsoft to deliver a unified data offering that addresses customers' critical data needs for Generative AI (GenAI). Specifically, the collaboration will see Neo4j's powerful graph capabilities natively integrated into Microsoft Fabric and Microsoft Azure OpenAI Service to seamlessly combine structured and unstructured data, and enable customers to uncover hidden patterns and relationships within their data for better insights and decision-making.

Sudhir Hasbe, Chief Product Officer, Neo4j, said "We're excited to combine Neo4j's unparalleled graph capabilities alongside Microsoft's seamless scalability, advanced AI capabilities of Azure OpenAI, and AI-Powered Analytics Platform with Microsoft Fabric. Enterprises can now unlock deeper insights, navigate complex data relationships, and drive better decision-making and innovation in ways that were not possible before. Together, we're helping customers redefine what's possible for their data in an increasingly interconnected GenAI world."

GitHub Copilot Enterprise Now Available

GitHub Copilot is now generally available, offering customers a customizable copilot tailored to their organization's code and processes. Developers face challenges deciphering and solving unique issues, bugs, or vulnerabilities in their codebase, reducing productivity. Limited access to institutional knowledge hampers creativity and productivity, hindering developers from fully leveraging their skills.

Just by integrating generative AI into the editor, GitHub Copilot has quickly defined a new age of software development, resulting in clear gains of developer productivity and happiness. GitHub is today bringing the next frontier of developer tools with the general availability of GitHub Copilot Enterprise–a companion that places the institutional knowledge of your organization at your developers fingertips. Now, team members can ask questions about public and private code, get up to speed quickly with new codebases, build greater consistencies across engineering teams, and ensure that everyone has access to the same standards and work that's previously been done. GitHub Copilot Enterprise comes with three core features:

Gain a deeper understanding of your organization's unique codebase. Copilot Enterprise streamlines code navigation and comprehension for developers, enabling faster feature implementation, issue resolution, and code modernization. It empowers junior developers to contribute quicker, assists senior developers in handling live incidents, and aids in modernizing aging codebases by offering clear code summaries, relevant suggestions, and quick answers to queries about code behavior.

2. Quickly access organizational knowledge and best practices. Copilot Enterprise integrates chat directly into GitHub.com, enabling developers to ask questions and receive answers in natural language on your codebase, and will guide them to relevant documentation or existing

Nutanix Names iValue Group National Distributor in India, Strengthening Channel Commitment

Nutanix has appointed iValue Infosolutions Pvt. Ltd. as the official value-added distributor for the Indian market. iValue Infosolutions is a prominent provider of integrated IT solutions and services in the Asia-Pacific region.

The partnership is a significant achievement for both entities as it combines Nutanix's leading hybrid multicloud solution with iValue's extensive range of enterprise applications and expertise in solution services delivery. It will help enable enterprises to expedite their digital transformation journeys and achieve optimal outcomes in their cloud environments.

According to Mordor Intelligence, the hybrid cloud market size is estimated at $129.43 billion in 2023, and it is expected to reach $348.53 billion by 2028, growing at a CAGR of 21.91% during the forecast period. The fifth annual Nutanix Enterprise Cloud Index report found that the hybrid multicloud usage in India stands at 12% presently and is expected to increase five-fold (to 63%) by 2026.

"We are delighted to welcome iValue Infosolutions into our esteemed distribution ecosystem. The alignment of iValue's top-notch IT solutions and services perfectly complements Nutanix's mission to help organizations run their applications in the environment that makes the most sense. We have high expectations for this partnership and believe that iValue's expertise will be invaluable in expanding our footprint," said Harsh Vaishnav, head – Channels at Nutanix India and SAARC.

CtrlS Unveils Upcoming Chennai Hyperscale **Datacenter Park**

CtrlS has unveiled their upcoming datacenter park in Chennai – their fifth hyperscale DC campus in India following Mumbai, Hyderabad, Noida and Bangalore.

CtrlS Datacenters will invest Rs 4,000 crore in the Chennai Datacenter Park, across phases. The company is expected to create about 500 direct jobs and over 9,000 indirect jobs.

Located in the Ambattur industrial area, the campus will include two datacenter buildings with a combined built-up area of almost 1 million square feet, and 72 MW IT load capacity.

The first datacenter building (Chennai DC 1) is fully booked, and will begin operations in Q2 2024. The second datacenter building (Chennai DC 2) is slated to be launched in the second half of 2024 – and is presently accepting bookings. Chennai DC 2 is a Ground + 10 floor structure, with an IT load of 27 MW.

The CtrlS Chennai DC Campus boasts of some advanced features such as:

Sridhar Pinnapureddy, Founder & CEO, CtrlS Datacenters, said, "We are delighted to unveil our upcoming Chennai DC Park. Chennai is the second largest datacenter market in India and holds strategic significance because of the presence of large number of subsea cable landing stations, coupled with the growing presence of enterprises and cloud service providers in the region."

iOPEX Launches ServiceNow Creator Workflow Add-On **for Compliance & Governance**

iOPEX Technologies introduces a new Compliance and Governance add-on for ServiceNow's Creator Workflows. It boosts ServiceNow's capabilities by integrating advanced compliance and governance features, including integrated risk management.

This add-on empowers organizations to proactively manage compliance and governance challenges within their ServiceNow environment. By automating compliance tasks, risk assessments, and reporting, the add-on ensures that businesses can adhere to regulatory requirements more efficiently and effectively. Features include streamlined compliance processes, enhanced risk visibility, and automated governance controls, all built on the flexible and powerful platform of ServiceNow Creator Workflows.

"Building custom apps and intelligent workflow automations that ensure all business procedures, operations and practices comply with legal standards, industry regulations, and internal policies is a growing requirement in the market as clients rush to digitally transform as much as possible.", said Craig Steel, Global VP ServiceNow – Creator Workflow.

"Our Compliance and Governance add-on, enriched with integrated risk management capabilities, signifies our commitment to providing robust, innovative solutions that address the complex needs of modern enterprises," said Shiva Ramani, CEO of iOPEX Technologies.

iOPEX's experience with ServiceNow allows them to leverage Creator Workflows to build custom solutions unique to an organization and business on the ServiceNow platform.

GEN AI

DATA QUALITY IS THE KEY TO GENERATIVE **AI SUCCESS**

Organizations Seek Decision on Harnessing Generative AI and LLMs

VINAY SAMUEL
CEO AND FOUNDER, ZETARIS

The quality of outputs created by generative AI applications and large language models (LLMs) is heavily determined by the quality of the data the models are trained on. This is why data is the most critical element determining the success of organisational generative AI projects.

When AI models are trained with poor quality, biased or incomplete data, they can generate spurious results. Like any computer system, generative AI is subject to the 'garbage in, garbage out' principle. No matter how well programmed the algorithms in the models are, training data quality remains the key determinant in how well these tools work in practical application.

When Microsoft launched its chatbot Tay in 2016, the importance of training data was laid bare. While there's no doubt the AI programming was excellent, Tay was allowed to 'learn' how to converse by using Twitter (now X) as one of its training data sources. Tay was switched off after 16 hours as the data it used from Twitter resulted in extremely offensive responses to questions. Tay's successor, Zo, was eventually discontinued for going too far the other way and avoiding potentially controversial topics.

These early forays into generative AI highlight the importance of data as a foundation of this emerging technology.

Public-facing AI models such as ChatGPT and Google Gemini (formerly Google Bard) highlight what can happen when AI models, even when trained with vast arrays of data, get it wrong. Those models can interpolate data to fill in blanks where their training data is incomplete. AI hallucinations occur when the training data has gaps, and the software tries to fill them in.

The corporate sector, government agencies and other organisations that want to leverage generative AI and LLMs are often faced with a decision. Should they invest their efforts in finding data scientists to help refine their models or put their focus on ensuring the data they feed their models is the most accurate and up-to-date possible? Given the choice between better data and more data scientists, better data will deliver a greater return on investment.

The challenge for organisations is not whether they have enough data to adequately train their AI models. The challenge is knowing where the data is and making it securely accessible to AI models. And the data must be made available to the AI models quickly so new or changed information is integrated promptly.

In most organisations, data is stored in multiple systems, each with their own structure and security. The data may reside in cloud services and other offsite locations, as well as within on-prem repositories. This dispersion makes it challenging using legacy approaches to data management to make information available to AI models.

A modern data preparation studio can make data available to LLMs and generative AI models in near real-time. Rather than copying data, which can be technically complex, time consuming and costly, a data preparation studio can make that data accessible to those models without duplication while respecting data governance and security frameworks.

When AI models and LLMs are trained with accurate and current data from your systems, the likelihood of errors and hallucinations is reduced.

While generative AI projects have a strong technical component, this does not remove people from the equation. It remains critical that any data that comes from a generative AI tool that is used for a business decision is vetted by a person. If an error is found, that needs to be fed back to the development team refine the model and remove any erroneous data.

The success of generative AI projects is strongly dependent on the quality of the data the models are trained with. By using a data preparation studio that enables information to be used without copying or increasing security risks, enterprise generative AI projects can be delivered faster and with less risk, enabling a faster return on investment.

NAVIGATING NEW FRONTIERS OF CYBERSECURITY

Cybersecurity threats intensified in 2023. Research at ISACA shows that 62% of organizations believe their cybersecurity teams are understaffed. As 2024 looms near, digital threats are expected to increase in sophistication.

BY SANJAY@ACCENTINFOMEDIA.COM

Over the past year, the Indian cybersecurity landscape was marred with enterprises witnessing some of the most damaging cyber-attacks and data losses with no sign of these threats slowing down. Amidst this, it is crucial, now more than ever, to recognize that while a security breach may not directly yield substantial user data loss, it has the potential to erode trust and drive customer attrition. Today, in the face of sophisticated threats such as phishing, ransomware, and intricate targeted attacks, organizations cannot risk navigating cybersecurity independently, necessitating reliance on a reputable vendor for support. In combination with the rise in cyber-threats, the scarcity of proficient cybersecurity experts is taking a deeper toll on the industry. Even

SUNIL SHARMA

VICE PRESIDENT – SALES, INDIA & SAARC, SOPHOS

"The strategic adoption of outsource cybersecurity services enables enterprises to proactively mitigate reputational damage and stay ahead of contemporary adversaries."

"83 per cent of cybersecurity and IT professionals in India are impacted by burnout and fatigue."

moreconcerning, according to the recent Sophos Future of Cybersecurity in Asia Pacific and Japan report, is that 83 per cent of cybersecurity and IT professionals in India are impacted by burnout and fatigue. In addition, 34 per cent of respondents said burnout and fatigue make them less diligent in their roles with 25 per cent identifying this as contributor to cybersecurity breaches.

Consequences of a Cyberattack

As a result of the complex threat landscape today, the concern shifts from whether an attack will occur, to when. Despite escalating threats, grasping the genuine toll of a cyberattack proves challenging, as gradual data breaches and underground market transactions emerge as typical, lingering aftermaths.

Moreover, accurately measuring the full cost of a cyberattack can present considerable difficulties. As per Sophos' State of Ransomware 2023 report, among Indian organizations surveyed that experienced a ransomware attack in 2022, the average recovery cost was an estimated US$1.82 million. However, this figure alone fails to capture the less tangible impacts of an attack, such as reputational harm and the loss of customers, both of which hold significant implications for businesses. Additionally, severe or persistent cyberattacks can foster prolonged concern and dissatisfaction among team members, resulting in diminished job satisfaction and increased employee turnover rates. Additionally, Sophos' The Future of Cybersecurity in APJ report outlines that 34% of surveyed cybersecurity professionals felt heightened levels of anxiety if subject to a breach or attack, with fear contributing to the high amount of burnout in the industry.

Furthermore, the Digital Personal Data Protection (DPDP) Act introduced by the Government of India has also enforced accountability on companies for 'failing to protect user data', imposing fines of up to 500 crore rupees depending on the magnitude and recurrence of data breaches suffered by the company.

With so many growing pressures on organizations to protect their operations, many realize they can't do it all on their own and are turning to cybersecurity as a service in the form of managed detection and response (MDR) to provide the defence they need. The strategic adoption of outsource cybersecurity services enables enterprises to proactively mitigate reputational damage and stay ahead of contemporary adversaries.

MDR providers deliver round-the-clock human-led threat detection and take proactive measures to avert cyber incidents.

The benefits of MDR

1. Superior cyber defenses – With MDR a business benefits from the breadth and depth of experience of the provider's analysts. An MDR vendor will experience a far greater volume and variety of attacks than any individual organization, giving them a level of expertise that is almost impossible to replicate in house.

2. Free-up IT capacity - Threat detection and response is time consuming and unpredictable. Working with an MDR service enables you to free up IT capacity to support business-focused initiatives.

3. 24/7 peace of mind - An attack can happen at any time. Adversaries are most active at times when an in-house IT team is least likely to be online, such as evenings, weekends, and holidays. By providing 24/7 coverage, MDR services provide considerable reassurance and peace of mind.

4. Add expertise, not headcount - Threat detection and response is a highly complex operation. Individuals in this space need to possess a specific and niche set of skills. This rare combination of competencies, exacerbated by a notable skills shortage, makes recruiting threat analyst expertise an uphill — if not impossible — task for many organizations. MDR services provide the expertise that enable organizations to expand their security operations capabilities without expanding headcount. 5. Improve cybersecurity ROI - Maintaining a 24/7 threat hunting team is expensive. By leveraging economies of scale, MDR services provide a cost-effective way to secure an organization and stretch its cybersecurity budget further.

The Secure Way Forward

As the threat landscape continues to grow and evolve, it is crucial to harness specialized expertise and threat intelligence offered by advanced cybersecurity solutions such as managed detection and response and incident response services.

MANUFACTURING THE WORST HIT BY RANSOMWARE **IN INDIA**

In India, the manufacturing sector has been the most targeted industry for ransomware extortion in 2023

Palo Alto Networks' Unit 42 recently released the Ransomware Retrospective 2024: Unit 42 Leak Site Analysis and Incident Response report 2024. As part of the Ransomware Retrospective, they studied 3,998 leak site posts from various ransomware groups. Leak sites are platforms where threat actors publicly disclose stolen data as a means of coercing victims into paying ransom.

Key findings from this investigation: Unit 42 saw a 49% YoY increase in multi-extortion ransomware attacks from 2022 – 2023 globally. In India, the manufacturing sector has been the most targeted industry for ransomware extortion in 2023. Of the 3,998 leak site posts from 2023 globally, LockBit ransomware remains the most active, with 928 organizations accounting for 23% of the total. LockBit is also the most active group in APAC and India (note: this was before the recent law enforcement disruption of LockBit). At least 25 new ransomware leak sites were observed in 2023; of which Akira led the way.

Anil Valluri, MD and VP, India and SAARC, Palo Alto Networks, said, "In India, the Manufacturing sector has emerged as the primary target for ransomware attacks over the past year. This unsettling trend underscores the critical vulnerabilities within the Indian manufacturing sector, where limited visibility into operational technology (OT) systems, inadequate network monitoring, and suboptimal cyber-hygiene implementation have left organizations exposed. Organizations must implement enterprise-wide Zero Trust network architecture to create layers of security that limit an attacker from successfully moving laterally around the network."

In a rapidly transforming country like India, organizations are constantly grappling with a blend of modern and legacy systems, creating huge cybersecurity gaps. And with attackers increasingly targeting software and API vulnerabilities, our findings come as no surprise. Thus, organizations need to move away from point-solutions that increase time to detect/respond and end up being more costly in the long-term. Fully integrated cybersecurity solutions will also do away with the idea of vendor sprawl, an issue that CISOs shouldn't concern themselves with during times of duress."

The 3,998 posts from ransomware leak sites represented a 49% increase compared to 2022, where 2,679 posts were observed globally. This increase can be attributed to zero-day exploits targeting vulnerabilities for MOVEit Transfer SQL Injection and GoAnywhere MFT, among others.

ANIL VALLURI
MD AND VP, INDIA AND SAARC, PALO ALTO NETWORKS

"In India, the Manufacturing sector has emerged as the primary target for **ransomware attacks over the past year. This unsettling trend underscores the critical** vulnerabilities within the Indian manufacturing sector, where limited visibility into operational technology (OT) systems, inadequate network monitoring, and suboptimal cyber-hygiene implementation have left organizations exposed."

As further evidence, when reviewing the number of compromises reported by ransomware leak sites, sporadic spikes were observed (see figure below). These loosely aligned with periods where ransomware groups began exploiting specific vulnerabilities.

Unit 42 2024 Incident Response Report: Speed of Exfiltration + Vulnerabilities Driving Activity

Unit 42 analyzed more than 600 incidents from 250 organizations for the 2024 Unit 42 Incident Response Report. This investigation went beyond ransomware leaksite posts into the overall casework volume. While phishing has historically been a popular tactic with attackers, the report found that it is declining, but only sort of.

From a one-third share of initial access incidents in 2022, phishing has dropped to just 17% in 2023. This indicates a potential de-prioritization of phishing as cybercriminals adapt to more technologically advanced – and perhaps more efficient – infiltration methods. More advanced threat actors are moving away from traditional and interactive phishing campaigns to less noticeable and possibly automated methods of exploiting system weaknesses and pre-existing credential leaks. Other key findings from the report include:

More-Sophisticated Threat Actors Are Gaining Initial Access Differently: There has been a discernible rise in the exploitation of software and API vulnerabilities. Exploiting such vulnerabilities accounted for 38.60% of the initial access points in 2023, up from 28.20% in 2022.

Threat Actors Grab Data Indiscriminately: In 93% of incidents, threat actors took data indiscriminately rather than searching for specific data. This is up from 2022, when 81% of cases involved non-targeted data theft. In 2021, it was even lower at 67%. The surge points to a growing

To access the complete article log on to:
www.enterpriseitworld.com

PIONEERING ZERO- TRUST SECURITY **WITH** BITDEFENDER ENDPOINT PROTECTION **AND GOPILOT AI INTEGRATION**

As businesses are operating in distributed teams with not much of tech fitness,' Enterprise IT World spoke to Anand Rajaram of GoTo to understand their strategy.

Can you elaborate on the concept of GoTo being an "all-in-one remote IT support hub"?

Businesses today, operating in distributed teams, often find themselves dealing with a lack of 'tech fitness,' resulting in IT inefficiencies, security vulnerabilities, and a pile-up of tech debt. The antidote is to build an environment where technology supports and enhances a flexible workplace spread across geographies, devices, and locations.

This is precisely where GoTo steps in with its pioneering 'all-in-one IT' approach. GoTo's commitment to being an all-in-one IT support solution is rooted in a profound understanding of the evolving landscape of flexible work. Our solutions integrate the most essential features and functions of IT support and management under a single pane of glass. Leveraging two decades of expertise in crafting support software that empowers flexible work, we've created flagship IT support solutions — GoTo Resolve and LogMeIn Rescue, used by customers worldwide.

GoTo Resolve embodies first of its kind zero-trust security architecture, endpoint protection powered by Bitdefender, mobile device management, and more. The recent infusion of GoPilot AI in Resolve is a game-changer. It not only expedites troubleshooting but also aids in crafting scripts and identifies problematic endpoints swiftly. On the other hand, LogMeIn Rescue revolutionises the IT support infrastructure for large enterprises. It is packaged to offer banking-grade encryption security with full account visibility with robust auditing and reporting. Moreover, its robust open APIs empower organisations to tailor integrations, build custom solutions and gives unparalleled data access. These solutions also play well in the ecosystem through their seamless integration with the existing tech stack—be it ServiceNow, Zendesk, MS Teams, Logitech, Salesforce, or Jira.

In essence, GoTo's all-in-one IT support solution is a testament to our dedication to enhancing productivity, resolving technical issues promptly, and ensuring optimal utilisation of time and resources of IT teams, achieved through combining the essential IT functions and integrations into one easy-to-use tool.

How does GoTo facilitate seamless issue resolution for IT agents compared to other support platforms?

At GoTo, our goal is to empower our customers' IT desks to channel their time and effort into more innovative and empowering initiatives, thus making IT more productive.

GoTo Resolve, a cost-effective solution for SMEs, serves as a unified platform consolidating all IT remote monitoring and management capabilities. This includes conversational ticketing, remote access, monitoring, multi-device support, and cutting-edge zero-trust security—all seamlessly accessible in one consolidated platform. Complementing this is LogMeIn Rescue, an enterprise-grade scalable IT administration tool designed to handle a spectrum of IT management challenges, from routine tasks to complex problem-solving. LogMeIn Rescue brings additional value by significantly reducing ticket resolution times. Technicians' complete tickets in 50% less time, freeing up 45 minutes each time an employee submits a ticket. The time savings on the IT side have implications for cost savings, more flexible staffing, and increased focus on other crucial technology-related projects.

We understand that every organisation is unique, and our flexible pricing and subscription plans cater to the diverse needs of different organisations and teams. This flexibility enables them to scale up or down as required, aligning with their growing business needs.

Can you provide examples of real-world scenarios where GoTo has proven to be effective in resolving IT issues seamlessly?

GoTo's effectiveness in resolving IT issues is evident in real-world scenarios such as the case of Quatrro Business Support Services (Quatrro BSS) who has been our customer for 10+ years. Quatrro Business Support Services (Quatrro BSS) is a global organisation specialising in providing cost-effective financial & accounting outsourcing solutions and technical support services for its 2,000+ customers (ranging from SMEs to enterprises across all industry verticals). Quatrro BSS required a remote solution capable of managing client infrastructure comprehensively in a hybrid environment while maintaining security and efficiency. By integrating LogMeIn Rescue, into their suite of technology solutions, Quatrro BSS achieved enhanced control over customer devices, increased transparency, and improved security. With its current suite of IT management and support technology including Rescue, the company's engineers are able to more efficiently solve customer problems which in turn help boost employee productivity, whilst at the same time increasing customer satisfaction by meeting or exceeding service level agreements.

In times of economic uncertainty, how do scalable and cost-effective IT solutions help organizations adapt to changing business landscapes?

In a landscape marked by economic uncertainties, the recent years have underscored a crucial lesson for CIOs and IT leaders: to build a resilient operational system. The strategic adoption of

ANAND RAJARAM
VP OF PRODUCT, GOTO

"By integrating LogMeIn Rescue, into their suite of **technology solutions, Quatrro BSS achieved enhanced control over customer devices** increased transparency, and improved security"

"In essence, GoTo's all-in-one IT support solution is a testament to our dedication to enhancing productivity, resolving In essence, GoTo's all-in-one IT support solution is a testament to our dedication to enhancing productivity, resolving achieved through combining the essential IT functions and integrations into one easy-to-use tool"

'all-in-one IT', consolidated solutions address this very need, offering a comprehensive approach that emphasizes cost-effectiveness, scalability, and security. In doing so, these solutions empower everyone from SMEs to large-scale enterprises to maintain competitiveness even in times of economic unpredictability, with the ability to grow as the business does. By investing wisely in scalable and cost-effective IT solutions, organisations not only navigate current challenges but emerge stronger, smarter, and resilient than ever before.

What challenges do businesses face when dealing with shrinking budgets, and how can IT solutions address these challenges?

Amid today's economic conditions, many businesses face shrinking budgets. This makes a perfect breeding ground for a myriad of IT challenges. One such hurdle lies in the hands of IT leaders, often left puzzled by the intricate maze of IT costs. This scenario, though challenging, presents opportunities for growth. IT leaders emerge as key players, equipped to unravel the intricacies of IT costs. By gaining a profound understanding of cost structures, they can overcome challenges associated with expense classification. This clarity not only brings transparency to IT budgets but also enables precise forecasting of future technology-related costs. Armed with this knowledge, businesses can make well-informed decisions, ensuring optimal resource allocation and building a tech-fit foundation.

If inspected more closely, the lack of consolidation in IT contracts results in increased costs and resource strain. Dealing with a multitude of contracts from various vendors introduces complexity and fragmentation into IT operations. Each contract may have its own set of terms, conditions, and service level agreements (SLAs), making it challenging to maintain consistency, visibility, and control over IT services and resources. This fragmentation can hinder collaboration, coordination, and alignment across different departments or business units, impeding organisational agility and responsiveness.

Which is why, IT consolidation emerges as a lifeline. By consolidating various IT functions and services under a unified platform, organisations can effectively streamline operations and do more with less.

ADAPTING TO EMERGING THREATS WITH AI-DRIVEN CYBERSECURITY

Amidst escalating threat landscape of cyber security, organizations are increasingly turning to artificial intelligence (AI) as a critical tool to bolster defence.

BY SANJAY@ACCENTINFOMEDIA.COM

The rise of cyber security threats in recent years has been unprecedented, fueled by technology advancements, increased connectivity, and the increasing sophistication of malicious actors. From ransomware attacks targeting critical infrastructure to data breaches compromising sensitive information, organizations face expanding range of cyber threats. The proliferation of Internet-connected devices, Cloud services and digital platforms has created new avenues for breach systems, as cybercriminals exploit vulnerabilities in software, networks, and human behavior to infiltrate systems and perpetrate attacks. The landscape has become complex with the emergence of state-sponsored cyber warfare and the easy access to hacking tools. Traditional approaches to cybersecurity, reliant on signature-based detection and manual intervention, are not sufficient to defend against the scale and complexity of modern cyber attacks. As adversaries evolve their tactics, organizations must embrace modern technologies to enhance defense capabilities and mitigate emerging threats effectively.

Artificial Intelligence (AI) has emerged as a powerful tool in combatting cyber security threats, strengthening capabilities to proactively deal with threat detection, rapid response and adaptive defense mechanisms. Machine learning algorithms can analyze vast amounts of data to identify patterns and anomalies quickly and enable security teams to respond to threats in real-time.

India is one of the most targeted countries in the world due to the sheer size and scale of its economy. For instance, total transactions processed by UPI in 2023 stood at 117.6 billion and total value UPI rails processed witnessed a little over Rs 182 lakh crore through the payments infrastructure last year while monthly transactions on UPI have seen an over 49% jump between January and December in 2023.

Also, geo-political factors mean that India is one of the most targeted nations. Speaking about the rising cyber attacks in India, Ratan Jyoti, CISO, Ujjivan Small Finance Bank, says, "India is an innovation hub dabbling with new technologies such as blockchain, AI, quantum computing and so naturally there are higher risks. Also, the surface area for attack become significantly more broader."

Digitalization is happening across domains in India due to national interventions with technology frameworks and regulatory environment that has spawned a huge ecosystem of start-ups. The overall environment in which the Governmental is pushing for digital and transparency has encouraged innovation even as it increases the risk quotient of all stakeholders.

"India's digital footprint is expanding rapidly. The sheer scale and size of India's digital economy means creates opportunities for frequent attacks and we also see a variety of attacks. In a way, this is good as it enables businesses to understand the spectrum of threats and better prepare to shore the defences," says Atul Kumar leading the government and global trade initiatives at Data Security Council of India (DSCI).

AI IS EMPOWERING ORGANIZATIONS TO FIGHT CYBER THREATS

Organizations are harnessing the AI to fortify cybersecurity strategies against threats including malware, phishing, and insider breaches.

"AI-powered security solutions can autonomously correlate and prioritize security alerts, augmenting human analysts' capabilities and reducing response times," says Binod Singh, CEO and Founder, Cross Identity.

The most common application of AI in cyber security is AI-equipped solutions are meticulously monitoring user and application behavior to swiftly detect signs of compromised accounts or malware infiltration. By analyzing patterns and anomalies, organizations can enhanced threat detection capabilities and take a proactive stance towards incident management before they can cause significant damage.

"From a product perspective, AI has become integral in cyber security management. Today more than 70% security products are AI-based. Adversaries are trying all the time with deception technologies and AI plays a crucial role in build a solution with deception mechanisms, like honeypot solutions," says Atul Kumar, DSCI.

Furthermore, advanced AI systems analyze network traffic, detecting suspicious patterns or activities such as distributed denial-of-service (DDoS) attacks or data exfiltration attempts. Organizations can fortify their network defenses and mitigate potential threats by identifying and

RATAN JYOTI
CISO, UJJIVAN SMALL FINANCE BANK

"The advent of GenAI, particularly the ability to generate synthetic data has empowered **organizations in threat detection and prevention activities. Traditional AI requires a very large** amount of data to train algorithms but GenAI enables to pick up clues and generate data to train the algorithm collapsing to speed the detection capabilities."

"India is an innovation hub dabbling with new technologies such as blockchain, AI, quantum computing and so naturally there are higher risks. Also, the surface area for attack become significantly more broader."

BINOD SINGH
CEO AND FOUNDER, CROSS IDENTITY.

"There will be increased focus on establishing AI governance frameworks and ethical guidelines for **the responsible deployment** of AI-driven cybersecurity solutions."

"AI-powered security solutions can autonomously correlate and prioritize security alerts, augmenting human analysts' capabilities and reducing response times,"

ATUL KUMAR
LEAD, GOVERNMENT AND GLOBAL TRADE INITIATIVES, DSCI.

"From a product perspective, AI is integral in cyber security management and more than 70% **security products are AI-based. Adversaries are trying all the time with deception technologies and** AI plays a crucial role in building a solution to combat deception mechanisms."

"India's digital footprint is expanding rapidly. The sheer scale and size of India's digital economy means creates opportunities for frequent attacks and we also see a variety of attacks which enables businesses to understand the spectrum of threats and better prepare to shore defences."

blocking malicious traffic in real-time.

AI technologies play a crucial role in addressing the complexities of cloud security by ensuring the proper configuration of permissions, access controls, and security settings. Through automated monitoring and enforcement of security policies, AI-powered solutions help safeguard sensitive data stored in cloud environments from unauthorized access or data breaches.

Fraud detection systems analyze user behavior and transaction data to identify anomalies or malicious actions, while ML algorithms detect patterns and deviations to thwart fraud attempts before they cause financial losses or reputational damage.

"The advent of GenAI, particularly the ability to generate synthetic data has empowered organizations in threat detection and prevention activities. Traditional AI requires a very large amount of data to train algorithms but GenAI enables to pick up clues and generate data to train the algorithm collapsing to speed the detection capabilities," says Ratan Jyoti, CISO.

CHALLENGES OF AI IN CYBER SECURITY

There are several challenges in incorporation AI into cybersecurity processes including issues with data quality, stemming from limited and biased datasets, which can lead to inaccurate results.

Worse, AI systems are susceptible to adversarial attacks. As people get used to the ease and convenience of AI-systems, relying too much on AI can reduce critical human oversight which is essential in security operations.

One of the fundamental concerns of deploying AI-driven cybersecurity revolves around the trade-off between privacy and security. AI's ability to process vast amounts of data raises concerns about excessive surveillance, prompting the need to fine-tune systems to minimize personal data collection while still effectively identifying threats.

The lack of transparency in AI models and concerns about privacy infringement make implementation challenging. Compliance with regulations such as GDPR requires significant expertise and resources and scarcity of skilled cybersecurity professionals compounds these challenges.

The integration of complex AI applications into cybersecurity operations raises significant moral concerns. Even as AI has demonstrated its effectiveness in defending against cyber threats, it also presents intricate ethical challenges that demand careful consideration.

ETHICAL CONSIDERATIONS OF AI IN CYBER SECURITY

Ethical considerations underscore the importance of thoughtful and responsible use of AI in cybersecurity. "There will be increased focus on establishing AI governance frameworks and ethical guidelines for the responsible deployment of AI-driven cybersecurity solutions," says Singh of Cross Identity.

AI algorithms may inherit biases from training data, leading to concerns about fairness and discrimination. In cybersecurity, biased AI could unfairly target certain groups, prompting questions about ethical profiling and discrimination.

The autonomous decision-making capabilities of AI systems raise accountability issues when errors occur and in then determining responsibility for mistakes—whether it lies with cybersecurity professionals, AI developers, or the organization—is complex and requires careful assessment.

Further, the opaque nature of some AI models pose challenges in understanding and justifying decisions. In cybersecurity, the lack of transparency can foster mistrust and uncertainty among security professionals, especially when explaining unexpected outcomes.

Beyond ethical considerations within the cybersecurity realm, the automation of threat detection through AI may lead to job displacement within the industry. This raises broader societal concerns about economic impact and the need to retrain and reskill to adapt to changing job roles.

Addressing these challenges requires ongoing dialogue and collaboration among stakeholders to navigate the complex moral landscape while leveraging AI to enhance security measures effectively.

AI IN CYBER SECURITY – THE NEED OF THE HOUR

The rise of cyber security threats in recent years presents unprecedented challenges, driven by technological advancements and evolving tactics of malicious actors. As organizations navigate this complex environment, the integration of AI in cybersecurity strategies has emerged as a powerful tool to bolster defenses with enhanced threat detection capabilities, rapid response mechanisms, and adaptive defense strategies to proactively safeguard digital assets.

However, incorporating AI into cybersecurity processes also has ethical considerations such as, data quality, adversarial attacks, transparency, accountability, and job displacement which must be addressed in a thoughtful manner in collaboration with stakeholders to harness the full potential of AI in managing cyber security.

REUBEN KOH
SECURITY TECHNOLOGY AND STRATEGY DIRECTOR (APJ), AKAMAI.

"As manufacturers use more APIs to enable **real-time production monitoring, predictive maintenance,** and cost optimization, they need to be more aware of the risks they are exposed to."

APJ MANUFACTURING SECTOR SUFFERS HIGHEST WEB ATTACKS AGAINST APIS

New research shows that manufacturing in APJ is the most targeted vertical, facing nearly one out of three (31.2 percent) of API attacks

BY SANJAY@ACCENTINFOMEDIA.COM

Akamai Technologies released a new State of The Internet (SOTI) report which highlighted that businesses, especially manufacturers in Asia-Pacific and Japan (APJ), are at great risk as cybercriminals continue to exploit APIs to conduct attacks.

Lurking in the Shadows: Attack Trends Shine Light on API Threats highlights the array of attacks that are targeting APIs and finds that 15 percent of overall web attacks in APJ targeted APIs from January through December 2023. The manufacturing sector in APJ is most at risk, having suffered the most API-targeted attacks across industries, attracting nearly one out of three (31.2 percent) of all web attacks. Akamai expects attacks to spike as the demand for API use increases, and strongly urges organizations to prioritize properly accounting for and securing their APIs – or risk suffering breaches.

APIs enable software, systems, and devices to communicate with one another, and are vital to most organizations because they have improved both employee and customer experiences. APIs are highly valuable to manufacturers as they enable the use of Industrial Internet of Things devices to increase efficiency, accelerate production, and enable real-time management of factories and inventories. Unfortunately, this digital innovation and the rapid expansion of the API economy have presented cybercriminals with new opportunities for exploitation. Successful attacks against APJ manufacturers can cause serious repercussions worldwide, given Asia's crucial role as a global manufacturing hub.

"APIs are increasingly critical to organizations, but they are also challenged with protecting APIs effectively, as security is often not properly baked into the rapid development and deployment processes of newer technologies like APIs," explained Reuben Koh, Security Technology and Strategy Director (APJ), Akamai. "As manufacturers use more APIs to enable real-time production monitoring, predictive maintenance, and cost optimization, they need to be more aware of the risks they are exposed to."

Lurking in the Shadows analyzes some of the most common problem areas regarding posture and runtime challenges. Other key findings of the report include:

The top sectors suffering the highest percentage of web attacks that targeted APIs were manufacturing at 31.2%, followed by gaming at 25.2%, high tech at 24.4%, video media at 24.0%, and commerce at 22.3%.

The top five regions with the highest percentage of web attacks targeting APIs were South Korea at 47.9%, Indonesia at 39.6%, Hong Kong SAR at 38.7%, Malaysia at 26.4%, and Japan at 23.4%. This was followed by India (19.0%), Australia (15.6%), Singapore (5.8%), the Philippines (5.5%), and New Zealand (4.8%).

In APJ, top attack methods include Local File Inclusion (LFI) at 16.8%, Server-Side Request Forgery (SSRF) at 11.8%, and Web Attack Tool (WAT) at 10.4%. Attackers are also favoring the use of newly surfaced vectors, like CMDi at 9.1%, which underscores that adversaries are continuously finding new methods and avenues to exploit targets.

Business logic abuse is a critical concern as it is challenging to detect abnormal API activity without establishing a baseline for API behavior.

To access the complete article log on to:
www.enterpriseitworld.com

GEORGE MOAWAD
COUNTRY MANAGER FOR ANZ, GENETEC

"What many hospitals lack is a single view of all the access activity that pulls **data from the different sources together and,** finds correlations that can indicate potential issues and provides meaningful alerts to security teams"

HOSPITALS CAN REDUCE RISK AND BOOST COMPLIANCE WITH **A UNIFIED SECURITY PLATFORM**

Unified Security Solutions: Safeguarding Hospitals Amid Complex Challenges

Hospitals and other healthcare facilities are extremely complex. The constant ingress and egress of staff and patients, requires strict access control and the need to be vigilant in case an incident occurs and escalates. This requires constant monitoring of different data feeds to protect assets and ensure patient and staff safety. Any failure in the system can result in a loss of trust and significant reputational damage.

For many hospitals, the challenge is not having systems in place to monitor all the different activity. As secured doors are opened using access cards, biometrics or other tools systems log the activity. Video cameras capture activity and can be used to investigate incidents. Locked secure cabinets holding medications can also be monitored using electronic access control tools.

A common problem in hospitals is the theft of medication. A recent report in The Medical Journal of Australiaconcluded that "substantial quantities of medications supplied to hospital wards and EDs [Emergency Departments] are not accounted for in electronic administration records." Data from four Melbourne hospitals recently found that about a fifth of medications that were unaccounted for were never given to patients. This represents a substantial cost as well as the risk of a drug-related incident impacting a hospital's reputation.

The challenge is not a lack of data. Hospitals and healthcare facilities have access to data from a variety of sources. What many hospitals lack is a single view of all the access activity that pulls data from the different sources together and finds correlations that can indicate potential issues and provides meaningful alerts to security teams.

Unless the data can be brought together and unified to generate useful information that drives insights, it's extremely difficult for security directors to maintain authorised movement through facilities, monitor drug theft, keep pollutants out of cleanrooms and protect patient records from prying eyes. For hospital operators, the complexity increases if they are responsible for a portfolio of facilities. Security directors need to be able track what is happening across all locations in real-time.

Access control systems are a critical element to overcoming these challenges. Access control solutions go beyond controlling flow of movement into secured areas. Access control systems can be used to ensure only authorised personnel can access sensitive equipment or cupboards where medications are kept. But, on their own, they can only tell a security team which swipe card was used to unlock a door.

When access control is unified with video surveillance operators can retrieve an access control event and correlate it with a video recording. This allows them to see if the person swiping the badge was, in fact, the authorised individual. As well as detecting potential theft, it ensures adherence with access policies and procedures.

With hospitals subject to a broad range of regulatory obligations, maintaining accurate logs can be challenging. As well as access information, it is critical that all incidents are captured. A video surveillance platform that not only stores video but applies machine learning to assist with detecting and alerting security teams to specific

To access the complete article log on to: www.enterpriseitworld.com

REDUCING INNOVATION FAILURES BY APPLYING STRATEGIC MANAGEMENT

One of the best ways to achieve cross-functional integration is to establish cross-functional product development teams composed of representatives from R&D, marketing and production

DR SURESH VIDYASAGAR MENON
CHIEF CONSULTANT & BUSINESS ADVISORY FOR SIX SIGMA, OPERATIONS, STRATEGIC MANAGEMENT AND INFORMATION SECURITY & DR SHWETHA KULSHRESHTA

ABOUT THE AUTHOR

Dr Suresh Vidyasagar Menon has 31 years plus of overall experience in IT, around 3 Years in Auditing of ISO 27001-Information Security Standard, has executed 25 plus projects in IT and two turnkey projects for eastern railways (Liluah) and has to his credit 14 publications in International Journals of Science, Engineering & Technology.

Although promoting innovation can be a source of competitive advantage, the failure rate of innovative products is high. Research evidence suggests that only 10 to 20% of major R&D projects gives rise to commercial products. It is nearly impossible to know prior to market introduction whether the new product has tapped an unmet customer need, although good market research can reduce the uncertainty about likely demand for a new technology, that uncertainty cannot be fully eradicated; a certain failure rate is to be expected.

One of the most important that managers can do to reduce high failure rate associated with innovation is to make sure that there is tight integration between R&D, production and marketing. Tight cross-functional integration can help a company ensure that:

Product development projects are driven by customer needs

New products are designed for ease of manufacture

Development costs are not allowed to spiral out of control

The time it takes to develop a product and bring it to the market is minimized

Close integration between R&D and marketing is achieved to ensure that product development projects are driven by customer needs.

Customers can be a primary source of new-product ideas. The identification of customer needs, particularly unmet needs, can be set the context within which successful product innovation takes place. Moreover, integrating R&D and marketing is crucial if a new product is to be properly commercialized- otherwise a company runs a risk of developing products for which there is little or no demand.

Integrating between R&D and production can help a company ensure that products are designed with manufacturing requirements in mind. Design for manufacture lowers manufacturing costs and leaves less room for error. Thus, it can lower cost and increase product quality. Integrating R&D and production can help lower development costs and speed products to market.

One of the best ways to achieve cross-functional integration is to establish cross-functional product development teams composed of representatives from R&D, marketing and production. The objective of the team should be to oversee a product-development project from initial concept development to market introduction. Specific attributes appear to be important in order for a product development team to function effectively and meet all its development milestones.

Leaders of the organization also must admit their own failures if they try to encourage other team members to responsibly identify what they did wrong and above all top management must bear primary responsibility for overseeing entire development process.

BPS AND SUPPLY CHAIN EVOLUTION: CHALLENGES & TRENDS

Unlocking BPS Success: Navigating VUCA with Key Trends

What are some of the key challenges that BPS providers face in today's complex business landscape?

In the past few years, the Business Process Services (BPS) industry has embraced challenges ranging from evolving customer demands and transformative forces unleashed by the pandemic to increasing supply chain complexities. They leveraged these challenges as catalysts for redefining the traditional BPS models. In fact, BPS was one of the industries that stood resilient during the pandemic, proactively adapting and embracing innovative ways to streamline remote working models, implementing digital advancements to empower the workforce with essential tools, and ensuring business continuity.

Some key challenges BPS providers grapple with today are keeping pace with rapid technological changes, talent management, and skills gaps, meeting evolving customer needs, uncertain economic conditions, and standing out in a crowded marketplace. Firstly, to stay ahead of the curve, embracing the relentless pace of technological evolution, especially in automation, analytics, and AI, is paramount. Secondly, the need for talent management and upskilling is accentuated by the imperative to navigate a digital world and empower the workforce for transformative roles. Thirdly, meeting client expectations, marked by a demand for hyper-personalized solutions, requires constant innovation and adaptability. Lastly, the economic uncertainty we face today adds layers of complexity, as the competitive environment necessitates a delicate balance of competitive pricing, value delivery, efficiency, and transformation to acquire new clients. Amid all this, agility and adaptability become the cornerstone for BPS providers to stay ahead in the race.

Can you provide examples of successful implementations where BPS providers have effectively delivered simple, scalable, and cost-efficient solutions?

BPS providers have consistently demonstrated their ability to drive industry-specific advancements through innovative solutions. There are innumerable examples of successful BPS implementations pioneered by many leading BPS providers using the right mix of people, process & technology.

At Mindsprint, we are committed to the core principles that emphasize the customer value proposition. Our approach revolves around ensuring controls and visibility, driving transformation through systematic process discovery, implementing tailored digital interventions, providing timely decision insights, facilitating access to talent, and optimizing costs.
A few examples of simple and scalable cost-efficient solutions we have successfully adopted are:

- **Touchless Solutions** eliminating manual efforts agnostic to ERPs, industries, markets, and business processes (Finance, Supply chain, HR services, etc..), leveraging new age technologies, delivering hyper efficiencies, and impacting business outcomes positively.
- **Citizen Developer programs** empower BPS talent, leveraging low-code/no-code technologies that significantly reduce development time and cost, minimize technical developer expertise involvement, and speed up time to market, thereby promoting self-service and innovation.

What trends do you foresee shaping the future of BPS, and how will providers continue to deliver value in increasingly complex environments?

Navigating the dynamic landscape of Business Process Services (BPS) in today's Volatile, Uncertain, Complex, and Ambiguous (VUCA) world requires a keen understanding of key trends that can be leveraged to deliver customer excellence. These key trends include Advanced Automation and AI for hyper-efficiencies, hyper-personalization to elevate customer experiences, adapting to hybrid working models supporting distributed workforces, and prioritizing Sustainability and ESG practices to meet evolving market expectations.

In response, to deliver enduring value, BPS providers should emphasize feverish adoption of Process Discovery solutions, anchoring transformation efforts in the ethos of "Discover to transform" that translates theoretical gains into tangible business results. Cultivating a continuous learning and upskilling culture becomes paramount in thriving within a digital-first paradigm. Furthermore, providers must proactively anticipate and respond to shifting client needs, market trends, and regulatory landscapes, ensuring they stay ahead of the curve and maintain a competitive edge in the complex business environment.

How are technology practices currently influencing the evolution of modern supply chains?

IThe global supply chain is going through a radical transformation fueled by cutting-edge technologies. This evolution from traditional supply chain to modern ways of managing supply chain driven by technologies and interconnected ecosystems isn't just about efficiency – it's about building a sustainable, transparent, and trustworthy ecosystem to manage various disruptions with minimal impact on business continuity. An amalgam of technologies is driving this change with AI & ML layers, propelling the speed of this evolution.

With data-driven insights and AI-powered digitalization, businesses can enhance inventory efficiency, logistics management, and teamwork, ultimately responding to client needs faster, optimizing costs, and building a more effective and sustainable digital ecosystem. Supply Chain Control Towers can significantly improve process controls, traceability, and real-time reporting.

GOPAL VENKATARAMANAN

HEAD OF BUSINESS PROCESS SERVICES, MINDSPRINT.

"Our approach revolves around ensuring controls and visibility, **driving transformation through systematic process discovery, implementing tailored** digital interventions, providing timely decision insights, facilitating access to talent, and optimizing costs.insights."

These technological practices greatly increase the effectiveness and agility of supply chains, ultimately improving customer happiness and commercial results.

What are some of the key challenges that traditional supply chain processes face in adopting new technology practices?

The pandemic and the consequent supply chain disruption made demand forecasting difficult and nearly impossible to estimate for manufacturing and inventory stocking. This has only been compounded by the geo-political tensions. The existing supply chain processes struggle to adapt to evolving market conditions and rapidly changing customer needs. Furthermore, the decentralized nature of global supply chains results in difficulties managing and accessing data, hindering timely decision-making. Additionally, the increasing capital intensity of supply chains raises concerns about achieving tangible benefits and return on investment.

When it comes to digital transformation, the selection of a suitable technology stack requires careful evaluation and needs to be fit-for-purpose yet build-for-change. Emerging technologies like AI, while promising, bring the risk of cybersecurity vulnerabilities that can compromise sensitive information and disrupt operations.

All in all, change management is a significant challenge when it comes to transforming traditional supply chain processes. One of the primary factors is the existing legacy infrastructure that many businesses have in place. The integration of new technologies often requires significant changes to these established systems, leading to complexities, potential disruptions, and resistance from stakeholders accustomed to the status quo.

How do these new technology practices impact supply chain efficiency and agility?

Amidst the dynamic landscape of supply chain operations, the integration of technologies such as RPA, IoT, data analytics, blockchain, AI, machine learning, and cloud computing is pivotal for enhancing efficiency and agility. As organizations navigate this evolving terrain, several key challenges and strategic solutions come to the forefront:

- **Global Trade Dynamics and Complexity:** The World Economic Forum projects that global trade flows will double by 2050. To navigate this increasing complexity, real-time technology upgrades and integrated systems are essential. This ensures smooth operations and end-to-end visibility and maintains necessary controls in today's competitive business environment.
- **Sustainability Challenges and Solutions:** According to ISO, the global logistics and transport sector contributes over a third of global carbon dioxide (CO_2) emissions. Digitization, including route optimization, consolidation, and smart warehousing, presents solutions to substantially reduce the carbon footprint, aligning supply chain practices with environmental sustainability goals.
- **Transparency Driving Trust:** As customers increasingly seek visibility into the journey of their products, Mindsprint emphasizes the adoption of blockchain technology. This aligns with Gartner's prediction that 60% of B2B supply chains will adopt blockchain technology in the next 3 to 5 years. This move enhances transparency and trust, crucial elements in meeting customer expectations and building strong business relationships.

Mindsprint strategically invests in shaping the future of its customers' supply chains. The focus is on delivering purpose-built solutions that enhance sustainability, efficiency, and transparency. Areas of focus are innovative digital procurement solutions, IoT-powered precision technologies, traceability, platform-led operations management, digital transportation management solutions, and more.

HOW ASIA PACIFIC ORGANISATIONS CAN BETTER NAVIGATE AI-POWERED THREATS, DATA PRIVACY AND SUPPLY CHAIN SECURITY CHALLENGES IN 2024

Looking further into the year 2024, Moshe Weis, CISO, Aqua Security identified three major threats that will continue to be top of mind for security teams globally and in the Asia Pacific region.

MICHAL LEWY HARUSH
CIO, AQUA SECURITY

"The democratisation of access to **AI has made the need for AI trust, risk and security** imanagement even more critical."

Worthy of first mention are AI-powered threats and mitigation. This is far from surprising with the increasing adoption of AI in both offensive and defensive cybersecurity strategies. As AI-driven threat actors become more sophisticated, organisations, too must deploy AI-driven security measures. More than ever, cyber defenders must stay ahead of these evolving threats through behavioural analytics, anomaly detection, and ethical AI practices.

The democratisation of access to AI has made the need for AI trust, risk and security management even more critical. These aspects of AI must be considered and organisations must evaluate the AI model, its application governance, fairness, reliability, robustness, security and data protection.

The attack surface of Gen AI is all over the AI lifecycle – from code to runtime. Therefore, security leaders will have to include in their security programs solutions and techniques for model monitoring, data and content anomaly detection, AI data protection, model management and operations, attack resistance and AI-specific application security.

Weis also pointed out that data privacy concerns will persist in 2024. As privacy regulations become more stringent, and user data protection gains importance, organisations are intensifying their efforts to navigate this complex landscape. They are not only focusing on compliance but also enhancing data security through encryption, robust access controls, and data anonymisation.

Lastly, Weis said that supply chain security remains a top concern and will deepen in 2024. He acknowledged that cyberattacks targeting the supply chain have the potential to disrupt businesses and even national security. As a result, organisations are increasing their efforts to assess and strengthen their supply chain security, recognising the need for robust vendor risk management practices and continuous monitoring to address these growing risks. Cybersecurity professionals must continue to adapt and innovate in order to proactively secure their organisations against modern, persistent threats.

The wisdom in prioritisation and remediation

As the threat landscape evolves so does the enterprise attack surfaces, and it continues expanding far beyond what most effective patch management programs can cover. The time has come for a forward-looking defence strategy that requires modernisation of the assessment tool portfolio. These tools must not only inventory patchable and unpatchable exposures, but also prioritise findings based on what an attacker could really do. To achieve that, they must validate the reality of the exposure based on the ability to penetrate existing security defences.

Gilad Elyashar, Chief Product Officer, Aqua reinforces the need for remediation. With sophisticated attackers being able to spin up in the cloud and launch attacks within a short period of time, it is paramount that organisations have the ability to quickly and proactively identify threats, prioritise certain risks when they get through, and know where to find them and stop them.

The conversations happening amongst CISOs are about reducing the attack surface. This shifts the conversation to not only seeing and blocking what is trying to get in but to stopping and responding to the things that do.

Personnel, budget constraints to spur demand for managed services

On the topic of what the current security landscape and tightening budgets mean to partners, Jeannette Lee Heung, Senior Director, Global Channel and Ecosystems, Aqua weighed in. She suggested that partners must navigate the intersection of heightened demand for advanced

cybersecurity and the constraints of tightening budgets. A notable trend is the acquisition of appropriate tools by customers to address their company's challenges.

Despite customers recognising the necessity of these tools, a prevalent challenge persists – finding the personnel with the requisite skills or expertise to fully leverage the technology they have invested in. Looking further into 2024, it is evident that numerous partners will be channelling investments into advisory and consulting services tailored to address specific customer needs. This foresight is driven by the recognition that the services market is poised for continued expansion.

As traditional partners are heavily reliant on the transactional model of reselling, they are at a crossroads. In response to the evolving landscape, they are likely to explore strategic options such as mergers, acquisitions, or forging partnerships with specialised services companies. This strategic shift is essential for bridging the gap between sustaining revenues and meeting the evolving needs of customers in the dynamic cybersecurity landscape.

Balancing cost, effectiveness, value and security

As cloud usage accelerates, organisations will increasingly have to find the balance between cost, effectiveness, value and security. To do that, more and more CISOs together with CIOs will look for consolidated platforms that can help CIOs and IT leaders manage cloud spend, security posture, asset configuration management, quality and cost optimisation.

As AI continues to be weaponised, it is essential for organisations in an increasingly complex and dynamic digital environment to have robust cybersecurity plans that are tested and proven effective. By staying informed and adopting innovative security solutions, businesses can navigate the evolving landscape of cloud native technologies with confidence.

"As AI continues to be weaponised, it is essential for organisations in an increasingly complex and dynamic digital environment to have robust cybersecurity plans that are tested and proven effective."

GEN AI

CLOUDFLARE AI FIREWALL: SECURING AI APPS AT **SCALE, FREE OF CHARGE**

Default AI Protections Shield Organizations from Attacks and Tampering

Cloudflare introduces Firewall for AI, offering protection against abuse and attacks targeting Large Language Models (LLMs). Leveraging its expansive global network, Cloudflare aims to safeguard LLM functionality, critical data, and trade secrets from the next wave of AI-based threats.

A recent study revealed that only one in four C-suite level executives have the confidence that their organizations are well-prepared to address AI risks. When it comes to protecting LLMs, it can be extremely challenging to bake in adequate security systems from the start, as it is near impossible to limit user interactions and these models are not predetermined by design – e.g., they may produce a variety of outputs even when given the same input. As a result, LLMs are becoming a defenseless path for threat actors – leaving organizations vulnerable to model tampering, attacks and abuse.

"When new types of applications emerge, new types of threats follow quickly. That's no different for AI-powered applications," said Matthew Prince, Co-Founder & CEO at Cloudflare."

With Cloudflare's Firewall for AI, security teams will be able to protect their LLM applications from the potential vulnerabilities that can be weaponized against AI models. Cloudflare will help enable customers to:

- Rapidly detect new threats: Firewall for AI may be deployed in front of any LLM running on Cloudflare's Workers AI. By scanning and evaluating prompts submitted by a user, it will better identify attempts to exploit a model and extract data.
- Automatically block threats – with no human intervention needed: Built on top of Cloudflare's global network, Firewall for AI will be deployed close to the end user, providing unprecedented ability to protect models from abuse almost immediately.
- Implement security by default, for free: Any customer running an LLM on Cloudflare's Workers AI can be safeguarded by Firewall for AI for free, helping to prevent growing concerns like prompt injection and data leakage.

According to Gartner, "You cannot secure a GenAI application in isolation. Always start with a solid foundation of cloud security, data security and application security, before planning and deploying GenAI-specific security controls." Cloudflare Firewall for AI will add additional layers to its existing comprehensive security platform, ultimately plugging the threats posed by emerging technology.

MATTHEW PRINCE
CO-FOUNDER & CEO AT CLOUDFLARE

"When new types of applications emerge, **new types of threats follow quickly.** That's no different for AI-powered applications"

SOPHOS

CRIMINALS EXPAND CRYPTOCURRENCY FRAUD GLOBALLY WITH SHA ZHU PAN KITS

After a thorough two-year investigation, Sophos X-Ops uncovers remarkable sophistication in investment scams deceiving victims

BY SANJAY@ACCENTINFOMEDIA.COM

Sophos uncovered a new cybercrime trend: "sha zhu pan" scammers are selling kits on the dark web, expanding globally. These kits, used for cryptocurrency fraud, originate from China and facilitate schemes like "DeFi savings."

Criminals position DeFi savings scams as passive investment opportunities that are similar to money market accounts, often times to people who have no understanding of crypto. Victims only need to connect their crypto wallet to a "brokerage account," with the expectation that they will earn significant interest from their investment. In reality, victims are adding their crypto wallets to a fraudulent cryptocurrency trading pool, which the fraudsters then empty.

"When pig butchering first appeared during the time of the COVID pandemic, the technical aspects of the scams were still relatively primitive and required a lot of effort and guidance to successfully scam victims. Now, as the scams have become more successful and the fraudsters have refined their techniques, we're seeing a similar evolution to what we've seen with ransomware and other types of cybercrime in the past: the creation of an as-a-service model. Pig butchering rings are creating ready-made DeFi app kits, which other cybercriminals can purchase on the dark web. As a result, new pig butchering rings that are unaffiliated with Chinese organized crime groups are appearing in areas like Thailand, West Africa and even the U.S.

SEAN GALLAGHER
PRINCIPAL THREAT RESEARCHER, SOPHOS

"As with other types of commercialized cybercrime, **these kits lower the entry barriers for cybercriminals** interested in pig butchering and vastly expand the victim pool"

"As with other types of commercialized cybercrime, these kits lower the entry barriers for cybercriminals interested in pig butchering and vastly expand the victim pool. Last year, pig butchering was already a multi-billion-dollar fraud phenomenon; sadly, the problem is likely only to grow exponentially this year," said Sean Gallagher, principal threat researcher, Sophos.

Sophos X-Ops has been tracking the evolution of pig butchering schemes for two years. The earliest iterations—dubbed by Sophos as "CryptoRom" scams—involved connecting with potential victims on dating apps and then convincing them to download fraudulent crypto trading applications from third-party sources. For iOS users, these scams required victims to download an elaborate workaround that allowed scammers to bypass security on victims' devices and gain access to their wallets.

In 2022, the scammers continued to refine their operations, this time finding ways to bypass app store review processes to sneak their fraudulent apps into the legitimate App Store and Google Play Store. This was also the year that a new scam pattern emerged: fake cryptocurrency trading pools (liquidity mining).

In 2023, Sophos X-Ops uncovered two vast pig butchering rings—one based out of Hong Kong and one based out of Cambodia. These rings leveraged legitimate crypto trading apps and created elaborate fake personas to lure victims and steal millions from them. Further investigation revealed that pig butchering operators were

To access the complete article log on to:
www.enterpriseitworld.com

NTT DATA & SCHNEIDER ELECTRIC COLLABORATE **ON EDGE AI INNOVATION**

Collaboration delivers the infrastructure needed to support demand of AI applications at the edge

NTT DATA and Schneider Electric launch innovative co-innovation, enabling enterprises to leverage edge computing. The partnership offers a solution integrating Edge, Private 5G, IoT, and Modular Data Centers, catering to computational demands of Generative AI applications at the edge.

The joint offering combines NTT DATA's Edge as a Service, which includes fully managed Edge to Cloud, Private 5G, and IoT capabilities, with Schneider Electric's EcoStruxure, a modular data center that fuses OT solutions with the latest in IT technologies. This powerful combination enables companies to maximize energy efficiency and meet the demands of compute-intensive tasks such as machine vision, predictive maintenance, and other AI inferencing applications at the edge.

"We've listened to our customers and know that processing vast amount of data generated by edge devices is where the future of digital transformation lies. That's why we're excited to announce that we have the solution to meet these obstacles and are ready to lead the way towards a more connected and efficient digital world." said, Shahid Ahmed, EVP New Ventures, and Innovation at NTT Ltd.

Shahid Ahmed
EVP New Ventures, and Innovation at NTT Ltd

"We've listened to our customers and know **that processing vast amount of data generated by edge devices** is where the future of digital transformation lies"

Customers can now implement a complete solution, including edge data centers tailored for digital transformation in remote and brownfield locations, where high compute demands critical infrastructure, such as power, cooling, racks, and specialized IoT and AI management systems.

The companies will go to market to address joint customer requirements to meet the growing demand from organizations who are looking to leverage edge compute to support automation and enable data-driven decision making. According to NTT DATA's Edge Advantage report nearly 70% of enterprises are accelerating edge adoption to solve critical business challenges.

With today's news, NTT DATA and Schneider Electric announced they are delivering the first Private 5G enabled deployment of an EcoStruxure Data Center at Marienpark Berlin. The historic site will be developed into a leading innovation park. The area spans over 30-hectare, equivalent to 74 acres, and will focus on delivering enhanced connectivity and compute experiences for users across the campus.

"Today's innovation ecosystems in Marienpark increasingly depend on specific technological infrastructures. Easy-to-access computational power combined with advanced connectivity are a key issue.," said Guido Schütte, Managing Director, Marienpark Berlin.

NTT DATA and Schneider Electric initially co-innovated to test the power of Private 5G at Schneider Electric's Lexington Smart Factory, the first of Schneider Electric's U.S. plants to become a Smart Factory showcase site leveraging Private 5G, IoT connectivity, edge analytics, and predictive analytics to drive energy efficiency and further sustainability goals..

ADDON NETWORKS TRANSCEIVERS: IDEAL FOR AI/ML APPS

Enhanced Data Center Capabilities for Industry Demands

RAY HAGEN
DIRECTOR OF PRODUCT LINE MANAGEMENT, ADDON NETWORKS

Our 800G transceivers are parallel **tested in our customers' environments to ensure** performance matches what is offered by the NEMs

AddOn Networks introduces a new lineup of 800G transceivers, facilitating AI, ML, and automation in data center applications. Compatible with InfiniBand and Ethernet, the range provides customers with a compelling alternative to NEMs for building and maintaining advanced optical networks.

Data centre operators need extensive data, storage and compute capabilities to ensure the enhanced speeds and low latency required to overcome growing industry demands. AI and ML tools optimise existing infrastructure and establish accurate data analytics for faster decision-making and increased automation. Yet the amount of bandwidth necessary for these to operate successfully, and the lack of compatible solutions in the market, makes selecting the right product a challenge. With this product launch, AddOn Networks will provide operators with the means to optimise their existing networks, alongside a premium support service and a reduction in part lead times.

"This family of transceivers mark an exciting new era for AddOn Networks," said AddOn Networks' Director of Product Line Management Ray Hagen. "Businesses operating in the data centre industry may already be aware of the benefits of 800G transceivers, but when ordering these directly through NEMs, they often experience long lead times and unnecessary delays in delivery. With our new range of transceivers, we will compress the timeline from order to delivery to ensure customers get solutions exactly when they require them. As a result, operators can maximise data centre output through AI and ML tools while making essential cost and time savings."

The transceiver range will enhance the handling and processing of bandwidth-intensive data flows when migrating from serial Central Processing Unit (CPU) based architecture towards parallel data flow in the Graphics Processing Unit (GPU). Once implemented within existing infrastructure, the transmission of data is accelerated, with additional capabilities to increase storage and compute capacity available to operators.

"Our 800G transceivers are parallel tested in our customers' environments to ensure performance matches what is offered by the NEMs," continued Hagen. "Our global leadership in third-party optics and expertise in testing means we can offer our customers not just a best-in-class transceiver, but a best-in-class service too."

AddOn Networks carries out 100% testing in its laboratory to guarantee the family of transceivers mirror the customers' data flows and their front-end environments to ensure full compatibility and performance while offering a lifetime warranty. As a result, customers can benefit from adaptable and reliable products, tailored to meet the specific demands of their data centre.

BY SANJAY@ACCENTINFOMEDIA.COM

Sridhar Pinnapureddy
Founder & CEO, CtrlS Datacenters

"With the government's ambitious plans for knowledge-based industries **and the resulting surge in digital transformation, CtrlS Datacenters is proud to contribute to Chennai's dynamic** digital landscape with its upcoming state-of-the-art datacenter campus"

CTRLS UNVEILS UPCOMING CHENNAI HYPERSCALE DATACENTER PARK

CtrlS Datacenters to invest Rs 4,000-crore in the Datacenter Park and create around 10,000 jobs through the ecosystem.

CtrlS has unveiled their upcoming datacenter park in Chennai – their fifth hyperscale DC campus in India following Mumbai, Hyderabad, Noida and Bangalore.

CtrlS Datacenters will invest Rs 4,000 crore in the Chennai Datacenter Park, across phases. The company is expected to create about 500 direct jobs and over 9,000 indirect jobs.

Located in the Ambattur industrial area, the campus will include two datacenter buildings with a combined built-up area of almost 1 million square feet, and 72 MW IT load capacity.

The first datacenter building (Chennai DC 1) is fully booked, and will begin operations in Q2 2024. The second datacenter building (Chennai DC 2) is slated to be launched in the second half of 2024 – and is presently accepting bookings. Chennai DC 2 is a Ground + 10 floor structure, with an IT load of 27 MW.

The CtrlS Chennai DC Campus boasts of some advanced features such as:

- State-of-the-art 230 kV on-campus gas-insulated substation (GIS)
- AI-Ready with advanced cooling technologies
- Earthquake resistant – Structurally designed to withstand earthquakes up to a magnitude of 7.5 on the Richter scale
- Flood-proof – Positioned 14 meters above sea level. The DC buildings are further elevated by 2.2 meters, mitigating flood risks
- 9-Layer physical security
- Building façade to have solar panels
- Planning for LEED Platinum-certification leveraging renewable energy and advanced water recycling amongst other sustainable initiatives

Sridhar Pinnapureddy, Founder & CEO, CtrlS Datacenters, said, "We are delighted to unveil our upcoming Chennai DC Park. Chennai is the second largest datacenter market in India and holds strategic significance because of the presence of large number of subsea cable landing stations, coupled with the growing presence of enterprises and cloud service providers in the region."

He further stated, "With the government's ambitious plans for knowledge-based industries and the resulting surge in digital transformation, CtrlS Datacenters is proud to contribute to Chennai's dynamic digital landscape with its upcoming state-of-the-art datacenter campus. We thank the Tamil Nadu government for extending all the necessary support and creating a conducive environment for setting up of our datacenters."

LEE KLARICH
CHIEF PRODUCT OFFICER, PALO ALTO NETWORKS

"As we continue to navigate the complexity **of the digital landscape, our commitment** to customers is unwavering"

PALO ALTO NETWORKS EMPOWERS CUSTOMERS WITH CORTEX PLATFORM FOR ENDPOINT SECURITY

New offer alleviates the cost of switching from legacy endpoint security solutions to Cortex XDR

Palo Alto Networks announced a new Cortex platform offer for endpoint security to help customers accelerate platformization and improve their endpoint protection.

Organizations struggle to prevent, detect, and respond to the continuous advancement of cyber-threats. To simplify their architectures, increase efficiencies and create better security outcomes, organizations are adopting platformization. The offer enables qualified customers to accelerate platformization and seamlessly transition to Cortex XDR by providing a "no-cost" period of the solution until existing legacy contracts expire. Additionally, the program includes a baseline package of "no-cost" professional services to assist with the agent migration.

Lee Klarich, Chief Product Officer, Palo Alto Networks, said, "As we continue to navigate the complexity of the digital landscape, our commitment to customers is unwavering. Today, we are building on that commitment by offering qualified customers a higher standard of endpoint protection through our new offer. Customers can now replace their existing legacy endpoint security solutions and seamlessly implement Cortex XDR without disruption."

Cortex XDR is the industry's most effective endpoint protection platform that identifies evasive threats with unmatched accuracy by continuously profiling network, user and endpoint activity with behavioral analytics. Cortex XDR accelerates investigations by providing a complete picture of every attack, automatically revealing the root cause of alerts. Palo Alto Networks was recognized in the latest Gartner MQ for Endpoint Protection Platforms underscoring its leadership position in the industry.

KYNDRYL

KYNDRYL TO TARGET A MARKET SIZE OF $530 BILLION

After Kyndryl being separated from IBM in 2021 as an independent technology service company, it has not only expanded its addressable technology areas but also enhanced its addressable market size. Enterprise IT World spoke to Rohit Sachdeva, VP-Account Management and Client Unit Leader, Kyndryl India to understand his perspective on India.

BY SANJAY@ACCENTINFOMEDIA.COM

How has Kyndryl's growth trajectory evolved since its separation from IBM?

Kyndryl has been on a remarkable growth trajectory since 2021, continually expanding the client base and strengthening our position in our existing accounts as the partner of choice.

As a leading technology services company, we doubled our addressable market opportunity to $530 billion and expanded our offerings horizon beyond specific technologies and platforms, which empowered us to create the best and most effective solutions to address the customers' challenges. Our go-to-market model is aligned with customer needs and domain requirements.

Kyndryl's strategy focussed on 3A's that is Alliances, Advanced Delivery, Account Focus—have yielded significant positive results.

On the Alliances front, our partnerships with cloud hyperscalers have proven highly successful. In the first nine months of this fiscal year, Kyndryl recognized an impressive $300 million in revenue tied to these alliances surpassing our initial hyperscaler revenue target, and raised our full-year goal to $400 million.

Advanced Delivery, powered by automation and AI-Ops adoption, has successfully transformed delivery for our clients from a manual reactive corrections mode to a proactive insight based automated remediations, resulting in higher system availability and generating an annualized savings of approximately $500 million.

Accounts-focused execution has helped realize $475 million of annualized benefits and we are on track to achieve the annual goal of $500 million.

Our evolving business mix is driving increased profitability. Kyndryl Bridge, our open integration services platform that harnesses AI to expedite automation and improve efficiencies, has enabled early adopters to realize substantial cost savings avoiding over $1 billion in annual costs. More than 750 global customers are operational on Kyndryl Bridge and is expected to cross 1000 by the fiscal year end. Kyndryl Consult, our technology consulting arm, is a critical part of our wider strategy that provides mission critical technology advisory, implementation, and integration services for customers. It enables us to meet businesses where they are in their digital transformation and provides a framework for flexible and iterative co-innovation.

We have also completed an internal transformation effort to transition to effective and efficient systems that drive fast, customer focused execution. This has built a streamlined future-ready operations model by moving to a platform strategy with industry-standard technologies and reducing our app count from 1,800 to a few hundred.

.

Could you elaborate on how Kyndryl's operations in India align with the national imperative of the 'Digital First' approach, particularly in the context of the 'Digital India' policy

Our work in India ties in directly with our national imperatives. Indian enterprises are prioritizing the 'Digital First' approach in their business strategy and we enable our customers to tap into the best talent and best solutions available to realize these goals.

Our skills focus extends to building strategic collaborations and programs with government bodies and NGOs. We have partnered with the Common Services Centres (CSC) under the Ministry of Electronics to run Cyber Rakshak, an initiative that will train over 100,000 women to become Cybersecurity Ambassadors within three years. We are working with IIT Tirupati to advance research, share knowledge, promote innovation and drive breakthrough developments in AI-enabled 3D-printing technology.

In Feb 2024, Kyndryl and the National Institute of Electronics and Information Technology (NIELIT) announced an advanced experiential learning initiative in DevSecOps, Cloud Operations, and Resilient Systems for 10,000 students across the country.

Kyndryl Collaborative Centres manages the vital systems of hundreds of customers around the world. A significant part of this talent base is in India whose advanced delivery capabilities are utilized to build customized solutions.

How is Kyndryl integrating AI into its operational framework, and what recent partnerships has it forged with hyperscalers in this domain?

Kyndryl is strategically and seamlessly incorporating AI into its solutions, aiming to provide our customers with enhanced efficiency and innovation. Our recent collaborations with major hyperscalers, including Google and Microsoft, have significantly bolstered these capabilities.

Kyndryl and Google Cloud have worked together since 2021 to help transform businesses with Google Cloud's advanced AI capabilities. In

ROHIT SACHDEVA

VP-ACCOUNT MANAGEMENT AND
CLIENT UNIT LEADER, KYNDRYL INDIA

"We are working with IIT Tirupati to advance research, share knowledge, promote innovation and drive breakthrough developments in AI-enabled 3D-printing technology."

February we announced the coupling of their in-house AI capabilities, including Gemini, with our expertise and managed services to develop and deploy generative AI solutions for customers.
With Microsoft, we are leveraging our Joint Innovation Centers, Kyndryl's growing patent portfolio in data and AI, and its access to Azure OpenAI to design, develop and drive new generative AI innovations and solutions across their enterprises. This also includes an AI-readiness program within Kyndryl Consult that provides customers with end-to-end services to explore and adopt gen AI solutions.
We employ AI in customer service engagements to expedite the categorization process, balancing automation with manual tasks. Kyndryl Bridge, our open integration services platform, uses AI to accelerate automation, drive efficiencies, and enhance security and resiliency.
Apart from the AI specific engagements, another key aspect of our cloud hyperscalers partnerships is a commitment to help our employees acquire valuable cloud expertise and certifications. In 2023, Kyndryls earned more than 32,000 cloud hyperscaler certifications.

Can you provide insights into Kyndryl's key customer base across various sectors such as healthcare, automotive, and banking?

Our proven track record in deploying cutting edge technology and leveraging global partnerships to deliver goal-centric solutions makes us a trusted partner for our customers.
In the telecom sector, we are working with a major telecom company to create a near-edge network across India for deploying applications that need real-time data processing.
For USDC, an online higher education services provider, we developed a state-of-the-art, cloud-based university management platform that provides personalized learner experiences, streamlines and optimizes learner onboarding, and enhances the administration processes of universities for greater operational efficiency and regulatory governance. With Honda Motorcycle and Scooter India (HMSI), we are driving IT modernization by managing infrastructure services, increasing uptime with automation, and enhancing resiliency. In healthcare, Dr. Lal Path Labs chose us to implement a cloud-based IT infrastructure to improve their agility, scalability, and security, enabling expansion into new markets.
We have longstanding and trusted partnerships with a majority of key players in the banking and finance sector. Earlier this year, Canara Bank chose us as their trusted partner to modernize their end-to-end IT operations and streamline services delivery across core banking, IT infrastructure, applications and network operations.
We are also working with Suryoday Bank to drive the bank's technology transformation program, improve operational efficiency, and increase digital banking adoption among its customers.
The National Payments Corporation of India (NPCI) has partnered with us to build a resilient and modernised next-gen private cloud infrastructure, migrate their datacenters and build a reliable and scalable platform capable of handling almost 15 billion transactions per month. Our Business Resiliency Services works with the National Stock Exchange to transition the NSE's IT into a modern, next-generation infrastructure and application landscape with built-in automation capabilities, improved security posture and resilience.

How does Kyndryl ensure the security and privacy of data while implementing AI solutions for its customers?

Our Responsible AI approach emphasizes the principles of transparency, fairness, and accountability to provide visibility into decision-making processes and data sources that build trust with our customers. Additionally, we actively detect and mitigate biases in AI solutions, aligning with our commitment to fairness and ethical AI design.
We deploy robust security measures, including encryption, access controls, and data loss prevention to safeguard against unauthorized access or misuse of customer data. This ensures that the data remains secure and confidential throughout the AI lifecycle. We also evaluate our vendor's data security practices and monitor them to ensure that they hold up to our stringent data security standards.

DAN FAULKNER,
CHIEF PRODUCT OFFICER AT SMARTBEAR.

"We are actively engaging in the recruitment, training,**and mentorship of software engineers, bringing technical** talent into the company's learning center of excellence.

SMARTBEAR ENHANCES **COMMITMENT TO INDIA** WITH INCREASED **INVESTMENTS**

New SmartBear DevOps Academy in Bangalore supports growing demand for skilled cloud engineers in the regio

BY SANJAY@ACCENTINFOMEDIA.COM

SmartBear, a leading provider of software development and visibility solutions, is increasing its investment in India as the market potential for software development solutions in the region continues to expand. SmartBear launched a new DevOps Academy, a best-in-class DevOps training program in Bangalore to prepare entry-level participants with the hands-on skills and confidence to be a successful cloud engineer. SmartBear is currently supporting more than 150 customers across India, representing fintech, health care, and transportation and logistics. The company opened an office in Bangalore in May of last year.

"The potential market for software development solutions in India is substantial and continues to expand rapidly as does the increasing demand for skilled developers and cloud engineers," said Dan Faulkner, Chief Product Officer at SmartBear. "We are actively engaging in the recruitment, training, and mentorship of software engineers, bringing technical talent into the company's learning center of excellence. SmartBear is proud to continue its commitment to India and the Bangalore community."

SmartBear received more than 4,000 applications for the 8-week paid DevOps Academy program that is based on two 2023 graduating classes of the company's successful SmartBear Developer Academy program in Poland and includes in-classroom, online, and practical learning designed for career progression at SmartBear. An immersive experience, SmartBear DevOps Academy offers project planning in collaboration with a diverse team, including developers, automation engineers, product managers, and UI/UX designers.

The successful Poland developer programs resulted in 91% of interns accepting full-time employee positions at SmartBear's Wroclaw office. Nearly 20% of the February 2023 class was women with the October class comprising 36% women. SmartBear is working with local universities and educational institutions in Bangalore as well as channel partners across the region to attract the best, most diverse new talent.

Upon successful completion of the program, participants in Bangalore will be assigned to one of SmartBear's award-winning product groups, including test management and automation, API development, and application stability. SmartBear is converging its toolsets this year into three integrated hubs – API Hub, Test Hub, and Insight Hub – for the industry's most comprehensive API development, testing, and production readiness. SmartBear has also been actively expanding its presence in India and the wider APAC region through strategic partnerships with local companies, most recently with Netpoleon India.

accops

#unlockfreedom75

ONLY SOLUTION YOU EVER NEED FOR SECURE REMOTE ACCESS

Free Licenses & Implementation*

4x reduction in support time

40% lower TCO in the long run

Keep your option ready with **Accops Digital Workspace**, the best alternative to your existing VDI.

- **Integrated & Comprehensive Offering**
  Remote access, application virtualization, VDI, MFA, identity federation, SSO & thin client: All in one.
- **No Multi-Vendor Dependency**
  Lesser downtime, quick resolution, rapid scalability, and easy security compliance.
- **Competitive Licensing**
  Flexible licensing with multiple options to choose from:
  • Perpetual or Subscription basis
  • Concurrent Users or Named Users
- **Contextual Security & Compliance**
  ZTNA-based access and restricted to trusted devices, networks, & locations, with unique out-of-the-box DLP features.

*75 licenses for the first year

Accops Systems Private Limited
3rd Fiesta, Old Mumbai Road, Baner,
Pune, Maharashtra 411045

Email: sales@accops.com
Phone: +918144880880

RNI NO: DEL ENG/ 2017/ 69906
Postal Reg. No.: DL-SW-01 / 4200 / 17-19

Date of Publication: 15 of Every Month
Date of Posting: 1 & 2 of Every Month