

THE REVIEW

MAY 2019

An in-house publication by Aptec – an Ingram Micro Company

Business insights for IT solution providers



DIGITAL SECURITY IN THE CONNECTED ERA

Empowering customers on seizing the digital opportunity

INSIDE

08

NetApp

Pioneering AI and analytics space for business growth

10

Microsoft

How Azure for IoT enhances digital transformation goals

16

Dell Technologies

How IoT is shaping the future of business

29

Micro Focus

Empowering Micro Focus Data Protection strategy in the AI and IoT era

INGRAM
MICRO



Contact Information

Aptec - GCC
 Innovation Hub Bldg. 1, Dubai Internet City
 P.O.Box 33550
 Tel: +971 4 369 7111
 Contact: Svetlana Sorokina
 Email: inquiry@ingrammicro.com

Aptec – Egypt
 KM 30 Cairo,
 Ismailia Desert Road,
 Al-Obour Investment Complex,
 Al-Obour City, Cairo, Egypt
 Tel: +202 24 77 21 53/54/57
 Contact: Mohamed Selim
 Email: Mohamed.Selim@ingrammicro.com

Ingram Micro – Lebanon
 St. Georges Square Blk A Floor 1
 Jal-EI-Dib, Beckanaya Str., Lebanon
 Tel: +961 471 8817
 Contact: Elie Abou Semaan
 Email: aptecblevantinfo@ingrammicro.com

Aptec – Oman
 Knowledge Oasis Muscat Building 4
 P.O.Box 100, Rusayl, Oman
 Tel: +968 9 642 9250
 Contact: Shivanand Palaniprasad
 Email: inquiry@ingrammicro.com

Aptec – Saudi Arabia
 Office 519, Akariya Bldg. 2, Olaya Rd
 P.O. Box 94609, Riyadh 11614,
 Saudi Arabia
 Tel: +966 11 460 1950
 Contact: Mohammed Sheikh
 Email: info@ingrammicrosa.com

Ingram Micro – Morocco
 Lot.33, La Colline 2, Immeuble les Alizés, Bureau
 302, Sidi Maarouf,
 Casablanca, Morocco
 Tel: +212 522 786 171 / +212 522 786 223
 Contact: Fouad Amrani
 Email: marketing-na@ingrammicro.com

Ingram Micro – Pakistan
 Ingram Micro Pakistan (Private) Limited,
 Suite# 1310, 13th Floor, Caesars Tower,
 Shahrah-e-Faisal, Karachi, Pakistan
 Tel: +92 21 3713 1961
 Contact: Hassan Shahid
 Email: inquiry@ingrammicro.com

Ingram Micro – Turkey
 Suleyman Seba Card
 82 / 3 Macka 34357
 Istanbul, Turkey
 Tel: +90 212 259 0064
 Contact: Hulya Erkmen
 Email: hulya.erkmen@ingrammicro.com

Published by
CPI MEDIA GROUP
 CPIMEDIAGROUP.COM



20 **VMWARE**
 Research from VMware has raised some fascinating insights into AI

22 **VERITAS**
 How Veritas is making it simpler for customers to access critical information across on premise, virtual or cloud infrastructure.

24 **IPSWITCH**
 How SMEs can leverage the key features of Moveit and WhatsUp Gold network monitoring.



29 **MICRO FOCUS**
 Micro Focus enlightens customers on how they can empower Micro Focus Data Protection strategy in the AI and IoT Era

38 **COFENSE**
 How regional customers and partners can thwart phishing threats effectively.

07 **APTEC NEWS**
 Ipswitch signs ME distributor agreement with Ingram Micro

Ingram Micro invests in building cyber security solutions offerings

Ingram Micro welcomes new director to head META Cloud business unit

Ingram Micro signs META distribution agreement with NVIDIA



08 **NETAPP**
 How the firm is pioneering the AI and analytics space for customers and partners.

10 **MICROSOFT**
 Why customers should opt for Azure for IoT to enhance digital transformation goals.

16 **DELL TECHNOLOGIES**
 Discover how the Internet of Things is shaping the future of business.

18 **APC BY SCHNEIDER ELECTRIC**
 APC by Schneider Electric's innovative offerings assist customers to capitalize on the benefits of Edge Computing and enhance operational efficiencies.



DR. ALI BAGHDADI

SVP AND CEO META,
INGRAM MICRO

To become a true AI-fueled organization, you need to fundamentally rethink the way humans and machines interact within working environments. Executives must consider how to deploy machine learning or deep learning to support data-driven decision-making.

Artificial intelligence will offer a multitude of benefits to your organization, however, only when viewed through a strategic business lens rather than as an IT project. One must identify the enterprise's main objectives, then align the AI strategy to achieve those outcomes. You may choose solutions that reduce costs, improve productivity, reduce risk, or extract greater meaning from data.

How can I use AI to achieve a competitive advantage?

AI is a broad category that includes natural language processing, computer vision, machine learning, and more. Consider your organization's vertical industry. For example, in the financial services, a firm may want to initiate its AI pilots by creating a robo-adviser or chatbot

Are You Ready to Harness the Potential of AI?

that can offer customers one-on-one investment advice.

How Can Deep Learning Help My Business?

The buzz phrase "big data" has been invoked repeatedly for several years. Most companies have jumped on that bandwagon. CEOs and CTOs recognized there was value in collecting all this data around their business processes.

That was phase one. Phase two was about finding more sophisticated ways to query that data – the basic business analytics trend. Phase three, brings Machine Learning techniques on the data. Machine Learning will help businesses develop models that are less backwards looking and more predictive in terms of outcome. Now, Deep Learning is the latest evolution of this incredible technology as it mimics the way our brain works. It will be more instructive when it comes to what to do or build or offer in your business.

So, what do you know about AI, ML & DL?

ARTIFICIAL INTELLIGENCE (AI): Artificial Intelligence is a technique which enables machines to mimic

human behavior. Ultimate aim of AI is to make intelligent machines that can perform human-like behavior and take its own smart decision. A machine completes tasks based on a set of rules that solve problems (algorithms). For example, such machines can move and manipulate objects, recognize whether someone has raised their hands, or solve other problems.

MACHINE LEARNING (ML)

ML is a subset of artificial intelligence. In fact, it's simply a technique for realizing AI. Training in machine learning entails giving a lot of data to the algorithm and allowing it to learn more about the processed information. The intention of ML is to enable machines to learn by themselves using the provided data and make accurate predictions.

DEEP LEARNING (DL)

Deep learning is a subset of ML; It is a technique for realizing machine learning. In other words, DL is the

next evolution of machine learning.

DL algorithms are roughly mimicking the information processing patterns found in the human brain. The brain usually tries to decipher the information it receives. It achieves this through labelling and assigning the items into various categories.

Whenever we receive new information, the brain tries to compare it to a known item before making sense of it—which is the same concept deep learning algorithms employ. Artificial neural networks (ANNs) are a type of algorithm that aim to imitate the way our brains make decisions.

For example, while DL can automatically discover the features to be used for classification, ML requires these features to be provided manually.

To learn more about the evolution of AI into deep learning, talk to Ingram Micro's AI team.

“**THE INTENTION OF ML IS TO ENABLE MACHINES TO LEARN BY THEMSELVES USING THE PROVIDED DATA AND MAKE ACCURATE PREDICTIONS**”



BAHAA SALAH

Managing Director, Gulf and Near East, Ingram Micro

Throughout my career, I remember going through several turning points - when I could see clearly that it was about time to change, adopt to new strategies, diversify, introduce new technologies to channel partners and their end customers and so on. I always fondly remember the times when I used to sell a notebook at two digits margin. It is incredible how far we have come today.

I believe we are now entering into another era, I believe it is time

“CHANNEL BUSINESSES CAN ENABLE DISRUPTIVE TRANSFORMATION FOR THEIR CUSTOMERS BY HAVING THE RIGHT KNOWLEDGE AND BEING ABLE TO REPRESENT NEW TECHNOLOGIES AND TRENDS.”

It's time for a change!

for a change again. Technology nowadays is not only about implementing a hardware, a software or an application. It has become essential to integrate solution-fulfilling business vision and strategic objectives. Throughout the past years, several companies have taken the turn towards digital transformation, not only to meet IT and internal users' needs, but more likely to integrate technology capabilities to transform their business. Technology is today an add-on to business models value proposition and a unique differentiator, offering the best-in-

class customer and user experiences, services, driving innovation and generating more profit.

My advice to my dear partners is to sell solutions and services; do not remain limited to products selling. Adopt to new technologies and include the same as part of a solution, like Security, IOT and AI, which are growing rapidly now. I have observed a faster adoption to these technologies, while in fact others expected these trends to take a longer time to resonate in this part of the world.

We, at Ingram Micro, are offering the best-in-class and the most

innovative solutions for these technologies and we support channel partners to shape up and to be able to represent different solutions in these domains.

Last but not least, end customers today are spending less in terms of traditional IT infrastructure. However they are willing to spend more in areas that will make them run their business better and add value to their existing setup. Therefore, it is critical that they adopt to new technologies, resulting in huge opportunities for channel partners. We encourage our partners to maximize these trends. ●





30 APR
01 MAY
2019
DUBAI WORLD TRADE CENTRE

#IngramAlEverything2019

Visit Ingram Micro and NetApp at Ai Everything 2019

Join us to know the latest technology updates and network with our leading vendors in the industry

 30th April to 01st May 2019

 Booth AIE010, Dubai World Trade Centre



APTEC ACCOLADES



Distributor of the Year 2018



Middle East Best
Distributor of the Year 2018



CCTV Distributor
of the Year 2018



CISO 50 Award for Virtual
Lab for Security Solutions



EMEA distribution partner
of the Year 2018



Distributor of the Year
for META 2018



Cloud Distributor of the Year 2018

Training Provider of the Year
for Cyber Security 2018

INGRAM MICRO SIGNS META DISTRIBUTION AGREEMENT WITH NVIDIA

Ingram Micro has announced a distribution agreement with NVIDIA, a world leader in artificial intelligence computing technology. With this agreement, Ingram Micro is authorized to sell and promote NVIDIA's Deep Learning, GPU Virtualization and High Performance Computing solutions in the GCC countries (namely, Qatar, Saudi Arabia, United Arab Emirates), Turkey and South Africa.

Tamer AbdelFattah, Head of IoT and AI Business Unit

in the META region said, "NVIDIA is a real pioneer of accelerating computing. Its latest GPU technology has a far-reaching impact on how today's enterprises manage, process and utilize data."

Carey Bowden, Head of Distribution EMEA, NVIDIA, said, "Ingram Micro's proficiency in supporting their customers' business transformations will help them take advantage of the exciting marketing opportunities represented by AI and visual computing."

INGRAM MICRO INVESTS IN BUILDING CYBER SECURITY SOLUTIONS OFFERINGS

Ingram Micro has announced a significant expansion of its Cyber Security business in Western Europe, Eastern Europe, Middle East, Turkey and Africa.

Ingram Micro is making meaningful investments to accelerate and reinforce its position as the go-to provider in EMEA for high value, speciality solutions, with Cyber Security being one of its first target markets.

Ingram Micro is establishing three Cyber Security centres of excellence (COE) covering the region, each providing specialized training, support, managed

services, solution architecting and consulting. The current Dubai COE will be joined by facilities in Eastern Europe and the Netherlands. Dr. Ali Baghdadi, Ingram Micro senior vice president and chief country executive META, will lead the company's new EMEA-wide Cyber Security division.

Baghdadi said, "We will leverage Ingram Micro's proprietary Cloud Marketplace, enabling customers to obtain subscription-based security services, while opening up more than three million active subscribers to our Cyber Security vendor partners."

INGRAM MICRO WELCOMES NEW DIRECTOR TO HEAD META CLOUD BUSINESS UNIT



Guruprit Ahuja has joined Ingram Micro as Cloud Director for META region. Ahuja will be replacing Rahul Bhavsar who has taken up a new role in Ingram Micro headquarters in Irvine, California, starting January 2019.

Ingram Micro established its Cloud business unit in the META region in November 2015 and in the last three years the company has built a strong foundation with awareness, transformation and strategy. Ingram

Micro established itself as a leader in Cloud business within a short period of time by rolling out the Cloud marketplace META, and has been continuously adding enhancements to help partners in the region to be more competitive.

Ahuja comes with 27 years' experience, holding key leadership roles promoting cloud computing platforms, data centre services and software solutions.

Ahuja said, "With my vast experience in Cloud, I am confident we will be able to further enhance our Cloud strategy and will add value to our partners and vendors."

IPSWITCH SIGNS ME DISTRIBUTOR AGREEMENT WITH INGRAM MICRO

Ipswitch, producer of secure file transfer and network management software, has announced a distributor partnership with Ingram Micro, one of the largest technology distributors in the META region.

Channel partners and resellers in the Middle East now have access to Ipswitch's MOVEit and WS_FTP for secure file transfer as well WhatsUp® Gold for network monitoring. Through this agreement, Ingram Micro is now authorized to distribute the

Ipswitch portfolio in 26 countries across the META, including Afghanistan, Algeria, Bahrain, Botswana, Egypt, Ethiopia, Iraq, Jordan, Kenya, Kuwait, Lebanon, Libya, Morocco, Namibia, Oman, Pakistan, Qatar, Saudi Arabia, South Africa, Tanzania, Tunisia, Turkey, Uganda, United Arab Emirates, Yemen and Zimbabwe. The distribution agreement may be expanded to additional regions in the future.

NEW VENDOR PARTNERSHIPS



Barracuda



BCDVideo



BlueJeans



Carbon Black



F-Secure



IDIS



Quanergy



Solarwinds



Suprema



Veer



LEVERAGING AI AND ANALYTICS FOR CHANNEL SUCCESS

Maya Zakhour, Partners and Pathways Lead, Middle East and Africa, NetApp, explains how the firm is pioneering the AI and analytics space for customers and partners.

Can you give an overview of how AI technologies have the potential to transform the work environment?

Artificial intelligence, particularly machine learning, is the ability to automatically learn and improve performance without the need to program it. It uses automation and available data in the system to generate information, making data an asset to the organization.



“NETAPP HAS ADOPTED A PARTNER-FIRST MODEL IN LINE WITH OUR CONTINUOUS INVESTMENTS BY PROVIDING TRAINING PROGRAMS AS WELL AS INCENTIVES. WE ENABLE OUR PARTNERS TO BENEFIT FROM STRONG, PREDICTABLE MARGINS, AND TO PROFIT FROM OPPORTUNITIES BY OUR RELIABLE BUSINESS MODEL.”

It can enable companies to accelerate innovation, achieve extremely high levels of performance and efficiency, as well as to provide highly personalized experiences for customers. It can practically be applied in many verticals – from financial services to healthcare and manufacturing.

Leveraging data expertise in a hybrid cloud world, NetApp uses AI and machine learning to constantly analyse and provide consistent insight across a data centre. It is essential to highlight that data management is crucial in running AI systems. The NetApp Data Fabric meets this requirement by simplifying and integrating data management across cloud and on-premises to accelerate digital transformation.

What is data analytics’ role in driving AI technologies?

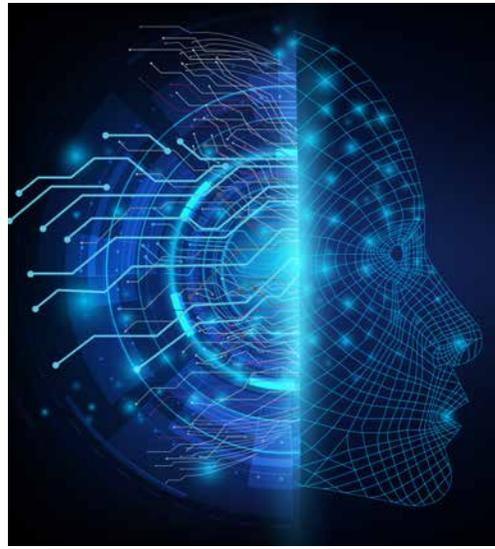
AI elevates data analysis to the point of completely eliminating human errors. Within a cloud environment, AI learns from historical data, identifies current patterns, and makes recommendations.

With AI, organizations generate data insights and can make recommended solutions for customers based specifically on data characteristics and insights. In turn, customers get recommendations best suited to their individual needs, with quick and efficient turnaround time.

What are the current challenges that partners face when looking to position AI technologies to customers?

Data governance, data privacy, data security, data quality and data management are all critical aspects in adopting AI and machine learning. The way an organization values data will determine the success of its implementation.

AI does not possess natural intelligence and therefore the system learns inductively by analysing data. If there is insufficient or flawed data input, then the analytic algorithms become non-predictive. Another concern is that setting up data infrastructure for AI can be expensive, especially as a hybrid cloud data-centric strategy plays an important role to its success.



How can channel partners enhance skills and play an essential role in helping customers in this space?

Digital transformation and AI have promoted businesses to upgrade their IT infrastructure and data management processes. To keep pace with the trends, channel partners will have to gain new essential skills through training and certification programs that align with the demands of AI and other next-generation technologies.

NetApp has adopted a partner-first model in line with our continuous investments by providing

training programs as well as incentives. We enable our partners to benefit from strong, predictable margins, and to profit from opportunities by our reliable business model. There is also an ongoing process to ensure that our systems are simpler and more efficient in terms of implementing quotes, orders, and the delivery of solutions.

Can you elaborate how NetApp is spearheading the AI and analytics space for customers and partners?

As data management remains a core aspect of AI growth, NetApp has created new types of solutions called NetApp ONTAP AI, powered by NVIDIA DGX™ supercomputers and NetApp AFF A800 cloud-connected all-flash storage.

The combination of a NetApp and NVIDIA architecture offer the world’s most powerful GPU solutions with the world’s fastest and most cloud-connected flash systems. ONTAP AI removes performance bottlenecks and enables secure, nondisruptive access to data from multiple sources and data formats. It is a more simplified solution that streamlines deployment with enterprise-grade data services and simple technology refreshes. It can handle more than 400 billion files with a single namespace.

Another feature of ONTAP AI is that it is scalable, and an enterprise can start small and grow as needed, as well be easily deployed without disrupting ongoing operations. ONTAP AI leverages the NetApp Data Fabric to unify data management across the pipeline with a single platform.

FlexPod AI is a converged infrastructure useful for private, public, or hybrid cloud strategies as it automates nearly all aspects of implementing an AI workload.

Additionally, it provides secure segmentation of resources ensuring data integrity within an AI or machine learning environment. Our focus is versatility and flexibility considering the characteristics of data which is diverse and distributed. Essentially, it is data pipeline capable to collect, clean, correlate, train, and model workloads. ●

BOOSTING MICROSOFT AZURE FOR IOT

Microsoft makes a case for why customers should opt for Azure for IoT to enhance digital transformation goals.

IoT has become—quite literally—an inextricable part of every aspect of our personal lives. While that's part of the beauty and fascination of modern technological advancement, it's also a cause for concern when it comes to data sharing and potential security breaches.

With the increasing involvement of IoT in our personal lives, it isn't enough to tell consumers to read the fine print. Those on the production side—developers and tech companies—and perhaps, eventually, policymakers, need to be responsible for ensuring that the IoT ecosystem is genuinely safe and secure for users.

The Internet of Things can deliver amazing value to organizations by reducing costs, increasing revenue, and transforming business.

But these IoT transformations are incomplete and unsustainable without a secure infrastructure, one that is protected from the physical devices and sensors to the services and data in the cloud.

The Internet of Things (IoT) is bringing together cyber infrastructure with the physical world. Cyber infrastructure includes Information Technology (IT) assets such as data storage, cloud services, operating systems, applications, various network technologies, backup services, monitoring, and security mechanisms like authentication, authorization, and auditing. The physical infrastructure includes devices and sensors of all shapes and form factors along with the control systems which ensure these elements function appropriately.

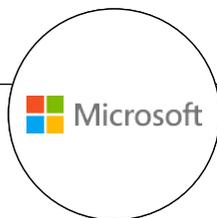
Why Azure for IoT?

Reduce complexity, lower costs, and speed up your time to market—all on the industry's enterprise-ready platform for the Internet of Things. Translate your digital transformation goals into action with the secure, open, and scalable Azure IoT.

Secure: Embrace security from the endpoint and connection to your data and apps, and through to the cloud.

Open: Use any device, OS, data source, software, or service, on-premises, at the edge, or in the cloud.

Scalable: Take advantage of one of the largest partner ecosystems and enable millions of devices and terabytes of data in most regions worldwide.



MICROSOFT AZURE PROVIDES A SECURE FOUNDATION ACROSS PHYSICAL, INFRASTRUCTURE, AND OPERATIONAL SECURITY. MICROSOFT INVESTS OVER A BILLION DOLLARS EVERY YEAR INTO SECURITY, INCLUDING THE SECURITY OF THE AZURE PLATFORM, SO THAT YOUR DATA AND BUSINESS ASSETS CAN BE PROTECTED.

TRANSLATE YOUR DIGITAL TRANSFORMATION GOALS INTO ACTION WITH THE SECURE, OPEN, AND SCALABLE AZURE IOT.

Why Azure's infrastructure is secure?
 With the challenges of recruiting security experts to maintain secure infrastructure, there is not a clear return on investment. To keep pace in this ever-changing security landscape, it's important that they can protect their infrastructure while also lowering their costs and reducing complexity. Azure is uniquely positioned to help with these challenges.

- 1. Microsoft Azure provides a secure foundation** across physical, infrastructure, and operational security. Microsoft invests over a billion dollars every year into security, including the security of the Azure platform, so that your data and business assets can be protected.
- 2. Secure network infrastructure**
 Adopting cloud helps you reduce infrastructure costs while scaling resources and being agile. Even though the network is shared, Microsoft has several mechanisms in place to ensure Azure's network and our customers' networks remain segregated and secure.

- 3. Secure hardware and firmware**
 Security controls are integrated into the firmware and hardware of Azure to ensure its secure by default and continues to be secure throughout its lifetime.
- 4. Secure testing and monitoring**
 Microsoft has over 3,500 cybersecurity experts who work on your behalf 24x7x365. This number includes over 200 professionals who identify potential vulnerabilities through red and blue team exercises. The red team tries to compromise Azure's infrastructure, and the blue team defends against attacks made by the red team. At the end of each red and blue team exercise, the team codifies what they've learned into the Azure operational security process, so the team becomes more effective at continuous detection and response.

Azure IoT Security Program
 Azure IoT Security Program For many businesses, securing both the cyber and physical aspects of their IoT infrastructure is complicated. It requires careful collaboration between device manufacturers, resellers, deployers, solution developers, cloud providers, and operators. The Security Program for Azure IoT addresses this need by providing security assessments, analyses, and recommendations for customers who are deploying an IoT solution. ●

THE FOUR REASONS TO USE ARTIFICIAL INTELLIGENCE



Tamer Abdel-Fattah, Head of IoT & AI Division, Ingram Micro Middle East, Turkey, and Africa describes four specific scenarios where customers must deploy Artificial Intelligence solutions to improve business efficiency.

Most customers today understand the significance of digital transformation and are willing to enhance their business by onboarding advanced technologies such as Artificial Intelligence (AI), Internet of Things (IoT) and blockchain. However, the trickiest part for end-users is in deciding when they need to deploy AI solutions and which solutions will have a genuine impact on their specific industry.

There are four main reasons why an organization must deploy AI solutions – if any one of them is applicable to your current situation, then you need AI solutions.

1. My business is supported by big operations that are affected by variable factors those change every day.

The nature of an organization's operation depends on the industry it caters to. It can be in the factory, warehouse, store, office, roads or on the web or mix of several different modes. With IoT solutions today, we can collect huge amounts of data about our assets and build AI solutions, keeping the ML/DL (Machine Learning or Deep Learning) engines always updated with the actual field data, allowing us to make better business decisions.

For example, ML is used heavily in logistics and supply chain management solutions today because it can take into consideration the huge amount of orders, resources (i.e. vehicles and their capacities, available machinery, workers, drivers, etc.), constraints (i.e. road conditions, vehicles capacities and service time, etc.) and SLAs, which are important criteria to archive data. The whole work orders management and planning can be done in minutes with ML, instead of hours and days. It also allows for using sophisticated ERP and CRM solutions, resulting in



Tamer Abdel Fattah
Head of IoT & AI Division, Ingram Micro Middle East, Turkey, and Africa

“THE MOST IMPORTANT POINT IS THAT THESE ML ENGINES ARE ADAPTING EVERYDAY WITH REAL CONDITIONS, WHICH MIGHT DIFFER FROM ONE WORK ENVIRONMENT TO ANOTHER.”

huge savings in the operations costs and reducing human error to a minimum. Can AI solutions also help in adapting processes even if a customer's operations are not related to the field services? Absolutely yes! RPA (Robotic Process Automation) solutions take care of this and can be coupled with digitization, which means legacy documents can be read even if they are written by doctors. Although, the error margin still exists similar to what a human does, it can be very helpful to boost one's digital transformation journey on the whole.

2. Early prediction is important to prevent downtime and continue my operations smoothly.

In many industries, machines are the most important assets. They have to be running all the time to maximize productivity. If one of the machines go down, the productivity will be negatively affected immediately for a long time until the problem is identified and solved. However, if you have a ML engine that can predict the same problem, it can give immediate work orders to solve the root cause before you reach to the downtime point. The scoring of some of these software ML engines can reach 99% accuracy. The most important point is that these ML engines are adapting everyday with real conditions, which might differ from one work environment to another.

3. High level of security is mandatory in my business.

When it comes to both cyber and physical security, Artificial Intelligence solutions have recently made a huge breakthrough to act like the human guard. The solutions can detect suspicious activity even if it is not able to identify exactly what the problem is. This way it can take action to stop the source of the suspicious activity and investigate further. It can avoid any unidentified threat before it affects your business drastically. Deep Learning is the only way to train machines to identify the features of a normal situation. When it comes to computer vision, the AI algorithms in the neural network can build a baseline to the normal activities in place and send immediate notifications in case of detecting any anomalies. With this we can convert CCTV solutions of just recordings to carry out video analytics after the problem has happened. This way AI solutions can be a real guard that can monitor hundreds or even thousands of cameras simultaneously and alert the right response at the right time. Also, if the threat is not one of the known

or identified ones, it doesn't mean that the AI-assisted cyber security software will not be able to detect it, unlike the normal cyber security solutions that don't have Deep Learning engine.

4. We are facing hundreds of customers every day to serve them

Customer-facing industries either directly or remotely serve customers on the Internet or via call centers. This is not an easy job as it requires a huge number of well-trained agents to deal with customers and effectively sell products or solve their issues. There are several solutions such as IVRs or availability of customer feedback pages on the Internet to enhance this process. However, it still leads to customer dissatisfaction largely due to lack of right options to select or delay on the phone while waiting for an agent to respond or delay in response after sending the complaint or feedback request on the Internet. Deep Learning chatbots are becoming a great solution today to simulate hundreds or even thousands of customer service agents who are available immediately and can understand your language using NLP (Natural Language Processing) technique. Recently, several companies have begun to dramatically reduce the number of customer service agents and increase the customer satisfaction level at the same time. The chatbot is already trained on your business and even enhances its learning every day.

If you experience any one of these reasons mentioned above, you need to get the help of AI/ML/DL solutions. At Ingram Micro, we have invested heavily in building the expertise in this specialty and our AI team can help you to know more and identify the right solution for your business. We have also announced our special distribution agreement with Nvidia to offer end-to-end AI solution for the first time in the Middle East, Turkey and Africa region. ●

IoT and AI Solutions

Ready Solutions



Supply Chain & Parcel Tracking



Cold Chain Management



Smart School Buses



Lynx Smart Vision



Indoor Tracking and Navigation



Connected Worker



Assets Tracking



Smart Machinery Management



Smart Ready Mix Management

Customized Solutions



Smart Public Transportation



Smart Connected Buildings



Smart Ambulances



Industrial Automation



Retail Analytics



Smart Environmental Systems



Intelligent Traffic Solutions



Smart Petril Stations



Smart Parking

Artificial Intelligence



Video Analytics



Connected & Autonomous Vehicles



Augmented Reality



Drones Technology



ALIA ATIYA

Senior Business Unit Manager,
Ingram Micro

Understanding IoT to guide customers

Alia Atiya, Business Unit Manager, Aptec - an Ingram Micro company, says it is critical for channel partners to educate and train themselves in the security risks associated with IoT adoption before positioning the solutions to end users.

The risks associated with IoT devices are derived from the original design of the IoT technology itself as it is relatively new; most of the IoT manufactures are truly not concerned about the security design of their products/devices as their highest priority is to deliver the technology to the market as soon as possible and as such this leads to thousands of IoT devices vulnerable to cyber adversaries. The second biggest risk is the nature of the technology itself whereby cyber security controls or feature sets cannot fit IoT devices due to the simple architecture and the hardware resource limitation to embed cyber security feature-set into them. For instance, a heating thermostat device cannot manage or run high computing security controls.

Regional clients often prefer to implement security controls around IoT devices as much as possible. The challenge is that global market offerings do not yet have tailored cyber security

offerings for IoT. We are seeing few inventions here and there, but we do not believe that the current market offerings are mature enough to address this challenge yet. Many customers will end up following the legacy IT security framework as a check-box for compliance, but the core issue is not addressed or resolved.

The market offerings for IoT technology is rapidly increasing, allowing customers a wide variety of choices. The most important aspect when it comes

to cyber security is the ability of the contractor or the supplier to implement a cyber security framework around the operational network if there are no controls built within the IoT devices. Visibility into the IoT operational network is key to understand the risk associated with operation and cyber exposure.

It is very important that the partners themselves understand the risk associated with IoT before clients' awareness campaign is launched, because often customers (end-users)

“IT IS VERY IMPORTANT THAT THE PARTNERS THEMSELVES UNDERSTAND THE RISK ASSOCIATED WITH IOT BEFORE CLIENTS' AWARENESS CAMPAIGN IS LAUNCHED.”

are usually more aware about the technology due to the early stages of its acquisition and adoption. Partners should work with their existing cyber security providers to understand the core challenges of IoT and OT networks before launching any awareness sessions as customers are keener to hear from partners about definite solutions for the problems. Partners have huge opportunities in this space and must maximize the prospects effectively, together with Ingram Micro. ●





HARD WON LESSONS FROM REAL WORLD IOT PROJECTS

Hani Khalaf discusses how the Internet of Things is shaping the future of business.

How can customers derive business value out of Internet of Things (IoT)? What kind of approaches do they need to adopt and implement within the organization to achieve this?

Internet of Things is a concept, not a “Thing” and it’s a tool in the Digital Transformation of businesses. We see the business value that customers can derive from IoT fall within four categories – Operational Efficiency (e.g. reducing the fuel cost of the fleet by 10%), Customer and Workforce Experience (e.g. personalization of

the shopping experience), Risk Mitigation (e.g. advanced computer vision on video surveillance cameras) and New Revenue models (e.g. all the new As-a-Service (aaS) business models). A strong commitment from top management for Digital Transformation is necessary. We advise customers to look at the Business Value derived from the IoT solution i.e. there has to be a Business Case to start with. The ROI has to be reasonable and it differs by vertical - e.g. in Energy Management and Optimization, we’re

seeing that a payback period of 3 to 5 years is acceptable. Our approach as Dell Technologies is to help customers derive value from the Edge to the Core to the Cloud.

Can you elaborate on the market potential of IoT in the region?

As many of our customers have embarked on their Digital Transformation journey, there is a huge interest in IoT, but IoT in the region is still in its infancy. It varies by country and vertical. For example, fleet management solutions in the UAE have become mainstream, where as we see big potential for the technology in Saudi Arabia. Because of the rising costs of Energy in the region, we’re seeing lots of interest in Energy Management and Optimization solutions, whether on a single building level, district and cities. Many cities in the region have started pilot IoT projects as part of their Smart City initiatives.

Are regional customers leveraging data to transform the way they do business?

Yes, we see many customers realize that “Data is the new Oil” and have embarked on projects to utilize their data to gain insights into the business. Big Data, Data Lakes and Data Science topics are on many customers’ minds and is essential when talking about IoT; IoT is an essential data source that customers can use to



Hani Khalaf, Business Development Manager – Internet of Things & Digital Cities Dell Technologies | Middle East, Turkey, and Africa (META)

enrich data analysis. We expect this interest to spike in the next few years as technologies such as machine learning, and deep learning become widely adopted.

What are the challenges that they have to first address before truly realizing the potential of IoT and data?

The biggest challenge we see is the ‘Business

“ IOT ENABLES CUSTOMERS TO DERIVE BUSINESS VALUE IN FOUR AREAS : OPERATIONAL EFFICIENCY, CUSTOMER AND WORKFORCE EXPERIENCE, RISK MITIGATION AND NEW REVENUE MODELS.”

Case’, i.e. having a validated business case for the IoT project, and this is an area we – Dell Technologies – can help with. We work with customers to analyze current business challenges, available IoT technologies and possible solutions. Other challenges we see are related to interoperability, security and manageability, where we can also offer solutions through Dell Technologies to reduce risk for IoT projects. When it comes to data, the biggest challenge we see is the availability of data and more specifically “clean data”. Again, Dell Technologies is very well positioned to help customers with the data collection, cleanup and analysis.

How crucial is edge computing for the future of businesses?

Edge Computing is extremely important, especially for IoT. The traditional model of (client

to Data Center) is not efficient in the IoT world. As IoT sensors and “things” generate lots of data, it’s neither efficient nor cost effective to transfer all this data to a data center. There is a need for an Edge Compute node near the data sources to read, interpret and analyze data before sending “useful data” only to a central location. Fast decision making at the Edge is another reason Edge Compute is the suitable model for IoT.

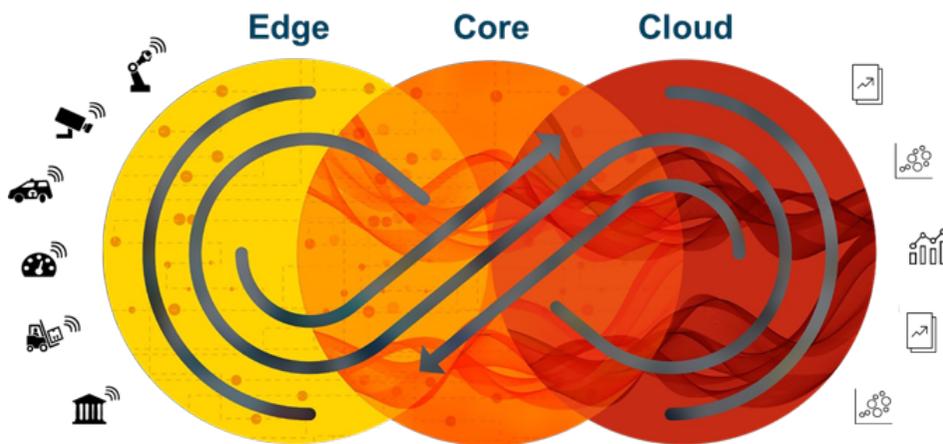
As there is increasing adoption for Artificial Intelligence (AI) in the market, we also see Edge becoming more important as the AI models will be running more and more on the Edge.

Can you discuss the growth of Dell Technologies IoT solutions division?

Dell Technologies announced in October 2017 the creation of the IoT Solutions division, with a \$1B investment through 2020. We’re leveraging a centralized strategy to tap into the broad capabilities of all seven independent, yet strategically aligned businesses in the Dell Technologies family – Dell, Dell EMC, Pivotal, RSA, SecureWorks, Virtustream, and VMware.

We are also continuing the evolution of our IoT Solutions Partner Program to help us qualify best-in-breed partners for different IoT use cases, as well as services from systems integration to deployment.

As a result, we have today a wide portfolio of IoT use cases – globally, in Transportation, Energy Management, Advanced Video Surveillance, Healthcare, Digital Cities and others. We continue to evolve the blueprints we create with our partners to ease the customer’s journey into the IoT World. ●



Dell Technologies: Making Things Smarter Across the IoT Ecosystem



KNOWLEDGE IS POWER

APC by Schneider Electric’s innovative offerings assist customers to capitalize on the benefits of Edge Computing and enhance operational efficiencies.

The rise of Edge Computing

Micro data centers are increasingly viewed as the appropriate response to the many challenges arising at the Edge. A micro data center is usually defined as a single-rack enclosure that can accommodate the IT equipment required to run the customer’s applications, while including all necessary power, cooling, security, and associated management tools (DCIM). The obvious benefits are faster deployment and increased standardization. This is especially true when IT and physical infrastructure manufacturers work together on reference architectures to provide plug-and-play solutions (i.e. Cisco HyperFlex and APC by Schneider Electric SmartBunker). Micro data centers are software-defined infrastructure that provide physical protection of the IT equipment and

remote management features. Because of the decentralized nature of IT Edge, effective and affordable monitoring is a key challenge. Cloud-based Datacenter Management as a Service (DMaaS) is the latest innovation in the industry that provides DIY installation and a subscription-based pricing model, which can be scaled up or down at any point in time. EcoStruxure IT Expert for instance, provides a secure monitoring platform that makes it possible to track on a single dashboard multiple IT racks and sites. Finally, it is worth to note that micro data centers provide sizeable savings over a centralized data center by eliminating the capital cost (materials, labor, and design) of the subsystems that are typically present in buildings (i.e. core & shell, raised floor, switchgear, generator, etc.). It also enables a “pay-as-you-grow” approach that helps

maximizing cash flow. To conclude, Edge computing is undoubtedly gaining momentum as use cases multiply, and we expect to see Distributed IT and micro data centers to be the bedrock of the ongoing new technology deployments. It is also interesting to note trends around compaction and remote management are transforming the UPS industry.

Connected Smart-UPS™ is here with FREE additional year of warranty

Innovation at your fingertips! SmartConnect is here, the first cloud-enabled smart UPS system. An easy setup enables you to instantly monitor and manage your power. With actionable alerts, critical notifications and RMM integrations, you get realtime data-driven insights with a click of a button.



Secure, remote monitoring



Pro-active lifecycle notifications



Cloud enabled as standard

APC's next-generation Connected Smart-UPS™ is more adaptable and easier to deploy than ever before, enabling you to view the status of your UPS through a secure web portal.

Through this intuitive remote management interface, you'll receive automatic notifications, firmware updates, and advanced support; providing you with added value - and more importantly - added peace of mind.

The Smart-UPS you've come to trust now offers Lithium-ion options

APC by Schneider Electric introduces the Smart-UPS with Lithium-ion

The world's most popular UPS is now available with Lithium-ion options. The Smart-UPS with Lithium-ion batteries offers trusted, premium power protection to ensure network and data availability. Designed for local edge environments and micro data centers, the Smart-UPS with Lithium-ion ensures consistent and reliable connectivity at the most critical moments.

2x the Battery Life - The Smart-UPS with Lithium-ion saves companies time and money by delivering two times the battery life compared with traditional lead-acid battery.

Efficient Installation - 30% lighter than lead-acid batteries, the APC Smart-UPS Lithium-ion enables a safer, faster and more simple installation.

Remote Management Options - Reduced maintenance and cloud-based remote management options make the APC Smart-UPS with Lithium-ion ideal for distributed environments and edge computing. Everything you love about Smart-UPS, now with lithium-ion. That's certainty in a connected world.

Build a profitable business and earn rewards

APC by Schneider Electric iRewards is a channel loyalty program designed to reward resellers.

Earn points on your APC sales and get rewarded!

Dream it. Earn it. Redeem it!

Follow the 3 easy steps to get going:

1. Become an APC Register or Select Partner by visiting your Partner Portal (www.apc.com/partnerpage)
2. Follow the link to iRewards and register yourself
3. Start earning!

Uniflair Access Floor- Available exclusively with Aptec

Uniflair™ Access Floor represents a reliable

and efficient choice because it significantly reduces management and maintenance costs by optimizing the connection of all infrastructure

over time: servers, racks, air conditioning systems, safety and monitoring solutions.

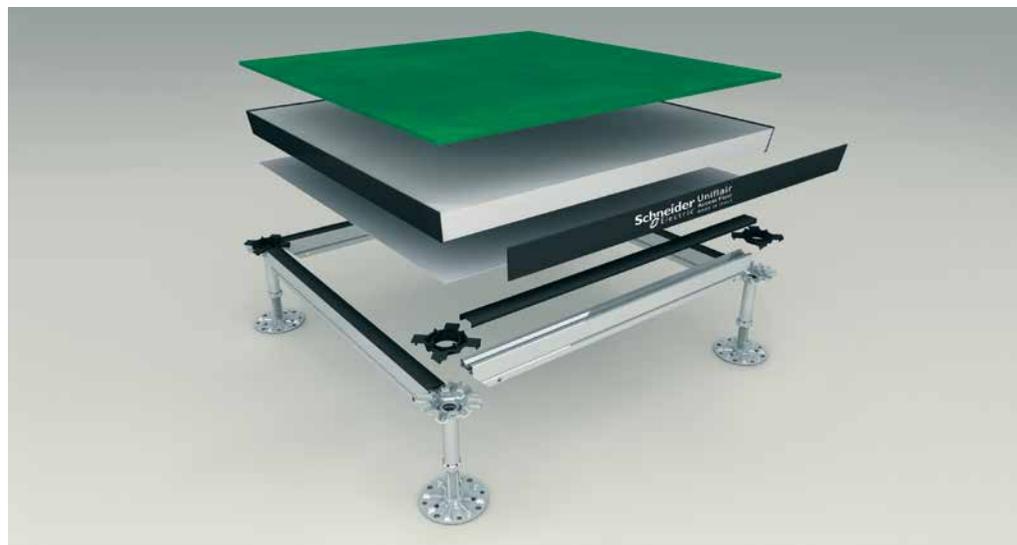
Panels

The panel, 60 x 60 cm, is made from a wooden chipboard core with a high-pressure plastic laminate finishing. The solution can be customized using different materials like calcium sulphate core with vinyl / rubber finishing.

Support structure

The galvanized steel supports with the steel frames along with support grid for the panels increase the mechanical resistance and the total stability of the floor.

Now available up to 600 sq. mt of both Calcium Sulfate and Wooden Chip board tiles in stock including the accessories





UNDERSTANDING AI

Research from VMware has raised some fascinating insights into AI

While consumers are increasingly using emerging technologies in their daily lives, they're also crying out for greater education from businesses and public authorities on the likes of Artificial Intelligence, blockchain and the Internet of Things (IoT). For many, the true benefits of these disruptive technologies are yet to be understood – with consumers seeing AI as the 'robot' from cinema, rather than a super-computing intelligence built into services to create improved, more immersive experiences across industries.

New technologies mean progress

According to a recent consumer survey (conducted in UK, France and Germany) from VMware, a leading innovator in enterprise software, technology is now at the heart of the daily lives of almost half (46%) of people, who recognize benefits in a multitude of areas. Fifty-three per cent, for example, realise this is driving a better customer experience with businesses, such as banks, retailers and doctors, while almost three quarters (71%) have faith in the power of these emerging

technologies to monitor their elderly parents at home alone. Consumers also believe in this technology's potential to improve environmental issues such as climate change (50%).

With such breakthrough technologies, however, comes the challenge of security and trust. Regarding new services and the use of personal data to support these, over two thirds (68%) of consumers admit they do not actually know who has access to their personal data. Sixty-six per cent, meanwhile, feel scared or nervous about banks having access to personal



Ihab Farhoud, Systems Engineering Director - METNA, VMware

50% ADMIT THEY HAVE A POOR UNDERSTANDING OF THESE NEW TECHNOLOGIES SUCH AS AI, THE INTERNET OF THINGS OR BLOCKCHAIN. FORTY FIVE PERCENT, FOR EXAMPLE

information about their lifestyle, such as purchasing habits, food, and travel – even if this is in support of better managing their finances.

Demand transparency and education

An element of confusion perhaps fuels these concerns; 50% admit they have a poor understanding of these new technologies such as AI, the Internet of Things or blockchain. Forty five percent, for example, believe Artificial Intelligence ‘is a robot’. In terms of addressing this, the majority think it is up to public authorities (50%) and businesses (53%) to help them understand these emerging technologies, and a way to do this is through better education and offering greater transparency.

As we approach a new digital frontier of technology, new opportunities emerge for businesses to drive innovation and positively impact our daily lives. There still remains room for greater education to fuel confidence in further innovation and adoption, and consumers have singled out the role of public authorities and companies to support this. Businesses, therefore, can seize the day – embracing these emerging technologies to deliver new and differentiated services to delight customers. With the right digital foundation, businesses can deliver on innovation now, and whatever is around the corner.

Money matters

Another fascinating insight gleaned from the research shed light on which aspects of their lives consumers are content for AI to look after. Consumers trust emerging technologies such as AI to care for elderly family members, but are wary of it managing their money.

Indeed, the research reveals how we want to let disruptive technology into our lives, and why businesses and the Government need to better educate all on its use and impact.

The populations of the three countries in the research appear to welcome the prospect of new tech that’ll improve their health and wellbeing. Three quarters (71%) of people are comfortable with it monitoring elderly relatives, allowing them to live longer at home. Those aged 55+ are the most receptive (74%), suggesting older generations believe the future of their family, and perhaps their own wellbeing, may no longer be best served by human hands. Additionally, almost half (47%) of those surveyed would be comfortable with their doctor having access to completely accurate data about their daily lives (drinking habits, rate of exercise, nutrition and diet) so that he/she can provide better advice on improving our health.

In sharp contrast, when it comes to our wallets, we want to maintain much more control. Just over a quarter (26 percent) would be happy having technology manage our finances, even if it resulted in more efficient saving. And just 7% would give Artificial Intelligence control over our money, even if it meant saving quicker for a house deposit. Additionally, while we are happy to give our doctor data on our wellbeing, 65% feel scared or nervous giving our bank access to data on spending habits, nutrition and diet, travel and commuting so that it can better manage our finances.

The findings reveal that while we show a real willingness to embrace a more tech-driven,

innovative future, half of people in UK, France and Germany don’t understand enough about new technologies.

People are looking to businesses and the Government to help educate them on the disruptive technologies that are out there, how they’re being used and the impact they’ll have on our lives. 53% of respondents say businesses have a role to play in helping them understand what these technologies do and how they can help. However, 64% don’t feel that businesses or the Government are currently clear enough on the technologies they use and how they use them.

With the majority of respondents (53%) saying that technology is already enabling a more immersive, improved experience with the companies they interact with, the benefits that the likes of AI, IoT and blockchain can bring to building customer relationships and brand loyalty is clear.

Europe has an illustrious history of innovation and as our research shows, people are still really willing to embrace innovation and new digital technologies if it improves their lives. As we approach a new digital frontier in terms of what technology can offer, the challenge for businesses and our government is to truly capitalise on it; delivering innovation to differentiate their service, excite customers and boost competitive advantage. This can only be achieved through a digital foundation that powers the apps, services and experiences that are transforming the world. With this, businesses can deliver the best of today and be the launchpad for tomorrow’s innovation.

About the survey

The research was undertaken between August and September 2018, interviewing representative samples of consumers in UK (2,000+), France (1,000+) and Germany (2,000+). ●



ROBUST COLLABORATIONS

With APTARE's IT Analytics, Mansoor Ibrahim, Distribution Success Manager – Middle East VERITAS, says customers will now benefit from enhanced reporting and analytics. Ibrahim says Veritas is making it simpler for customers to access critical information across on premise, virtual or cloud infrastructure.

CAN YOU ELABORATE HOW THE APTARE ACQUISITION WILL STRENGTHEN VERITAS' BUSINESS?

APTARE's technology will allow Veritas to offer customers an enhanced analytics platform that provides deep insights and reporting across their different data protection, virtual infrastructure and storage environments. It will enable customers to:

- Gain visibility into their complete infrastructure—on-premises and in any cloud—to make more informed decisions.
- Have a common reporting platform from

tape to disk to cloud, which is essential in a multi-cloud environment.

- Better anticipate needs and predict outcomes, such as optimizing their infrastructure, reducing costs, and meeting compliance and SLA requirements.

The addition of APTARE's IT Analytics solutions to Veritas' product portfolio also strengthens the company's product integrations with key cloud and technology providers including VMware, AWS, Microsoft Azure, OpenStack and ServiceNow.

HOW CAN REGIONAL CUSTOMERS DEVELOP ADAPTIVE INTELLIGENCE INTO THEIR OPERATIONAL AND EXPERIENCE APPLICATIONS THROUGH HYBRID CLOUD?

The industry's first end-to-end open analytics platform gives customers a view into all their data, no matter where it resides. Today, the protection and management of business data in most organizations is split across many different tools and technologies. As organizations move data and workloads to the cloud, they face major challenges locating their data, migrating it simply and cost-effectively, and protecting it

“
WE’RE MAKING IT SIMPLER FOR CUSTOMERS TO ACCESS CRITICAL INFORMATION ABOUT THEIR INFRASTRUCTURE AND PROVIDING THEM WITH A ONE-STOP SHOP FOR ALL REPORTING REQUIREMENTS.”

in all environments. With new data privacy laws coming into effect, organizations globally must also have the ability to see, access, protect and manage their data—no matter where it lives.

HOW WILL VERITAS ENABLE END USERS TO LEVERAGE THE BENEFITS OF ON-PREM AND CLOUD IT ANALYTICS?

APTARE is a global leader in analytic solutions for both on premise and hybrid cloud environments and helps organizations mitigate the risks of their business data by identifying unprotected data, stressed storage resources or compliance risks, wherever the enterprise data resides – on-premise, in hybrid, private or public clouds. With APTARE’s IT Analytics, Veritas customers will now benefit from enhanced reporting and analytics across NetBackup and other third-party applications. We’re making it simpler for customers to access critical information about their infrastructure and providing them with a one-stop shop for all reporting requirements—on premise, in any cloud and across their technology ecosystem. APTARE’s vendor-agnostic approach to data analytics is pivotal to the enterprise management framework for managing the modern enterprise IT structure. It drives cost savings, allows a healthy storage environment and comprehensive reporting with deep analytics, and presents IT professionals with every metric needed to ensure their data is protected and recoverable.

It gives a balanced approach to moving our portfolio forward through both organic and inorganic growth – Veritas continues to

innovate and develop solutions internally while also looking for opportunities with existing technologies that accelerate our vision.

HOW CAN BUSINESSES STREAMLINE UNSTRUCTURED DATA AND GAIN ACTIONABLE INSIGHTS?

Data volumes continue to grow at an alarming rate in many organisations – with much of the data growth coming in unstructured or semi-structured data repositories. And often, organisations have little visibility into this data: on average, more the 50% of the data in any organisation is “dark” – that is, its value is unknown. Organisations need more insights to their data, to both extract the promised value and protect against risk.

Data regulations continue to expand and evolve across countries (GDPR in the EU, POPI in South Africa, or KVKK in Turkey) and industries (MiFID, HIPAA), and challenge the way in which organisation manage data. Since GDPR has been implemented, fines totally \$56M have been issued in more than 200,000 cases, but watchdogs have said they’re just warming up.

Veritas helps organisations gain more insights to data, reducing risk and cost by providing automated capability to find, filter and act on the data. Veritas is unique in having a broad set of market-leading data governance offerings, covering file analysis, data archiving and retention, and eDiscovery, all incorporating the same powerful data classification engine.

And now, with the addition of APTARE to the Veritas portfolio, we can provide more insights into our customers’ backup, storage and cloud environments, too.

HOW CAN REGIONAL PARTNERS PLAY A ROLE TO ASSIST CUSTOMERS TO USE ANALYTICS EFFECTIVELY?

Three concepts - protection, availability and insight - are at the heart of what Veritas does. Understanding and managing a robust data-protection policy is paramount to achieving long-term success and operability. Having a strong library of points-in-time for recovery not only builds an attainable recovery point against malicious attacks like ransomware but also provides a plan for restoration due to infrastructure instability, system outages and



Mansoor Ibrahim, Distribution Success Manager – Middle East VERITAS

even human error. Backups create the ability to travel through time and return to a functional state; however, the strategy doesn’t end there.

Using multiple storage destinations and formats adds to the resiliency of your backup infrastructure. Whether it’s a combination of tape, secondary disk storage or cloud storage, having a robust timeline of backups spread across multiple locations ensures that when the unexpected hits, you always have a point of recovery available. A healthy number of backup copies located in online and offline media allows for resilient and rapid recovery from any recovery scenario.

Partners can demonstrate the value to their customer install base by understanding the importance of data protection.

The addition of APTARE’s IT analytics platform offerings to the Veritas product portfolio enables Veritas to provide full-stack insights, analytics, and reporting for our data protection products including NetBackup, Backup Exec, and InfoScale. It will provide customers with historical tracking and trending, real-time dashboards, future forecasting, and predictive analysis of their enterprise data protection environment. ●



GAINING EFFICIENCY

Matt Scotney-Jones, Regional Channel Sales Manager, EMEA, Ipswitch, elaborates how small and medium businesses can leverage the key features of the firm’s flagship secure and managed file transfer software – Moveit and WhatsUp Gold network monitoring.

Can you elaborate on the main elements that customers must consider when sharing data?

There are several aspects customers must consider - Is the data encrypted at all stages (i.e., both in transit and at rest)? Is the network upon which that data is shared fully secure? Did the recipient receive the data? Can you prove this? Do you have a tamper-evident audit trail that can be used to prove compliance with relevant regulations? Are there any processes in place to prevent human error or to ensure the identity of users?

How does Ipswitch address the challenges surrounding data sharing through MOVEit?

MOVEit encrypts all data from end-to-end and has a number of features that ensure complete control over who can access shared data including multi-factor authentication (MFA), a hardened platform, a completely tamper-evident audit trail, an alerting system that notifies administrators of failed transfers and more. MOVEit also includes capabilities to extend secure data sharing beyond administrators such as Secure Folder Sharing and Ad Hoc for end users.

What are the security aspects that MOVEit guarantees customers?

Advanced security features include FIPS 140-2 validated AES-256 cryptography, file integrity checking, user authorization/authentication, delivery confirmation, non-repudiation and hardened platform configurations. MOVEit logs activities in a tamper-evident database to comply



Matt Scotney-Jones, Ipswitch

with ISO 27001, HIPAA, PCI, GDPR, SOX, BASEL I/II/III, FIPS, FISMA, GLBA, FFEIC, ITAR and data privacy laws. It also integrates with your existing DLP and anti-virus systems, identity systems through SAML 2.0, AD, LDAP services, and SIEMs. Edictally, MOVEit supports available failover and disaster recovery options to ensure uninterrupted service at all times.

How can businesses monitor its entire network infrastructure through WhatsUp Gold network monitoring software? What kind of market demand have you observed from regional customers?

WhatsUp Gold continuously monitors the availability and performance of an organization’s infrastructure from routers, switches, and

firewalls through to servers, storage devices and applications and VMware and Hyper-V virtual machines. In short, WhatsUp Gold can monitor anything with an IP address that can be accessed with standard monitoring protocols including ICMP, SNMP, WMI, and SSH. WhatsUp Gold automatically discovers, maps and monitors cloud environments including Amazon Web Services and Azure servers allowing administrators to monitor, report and alert on the status and performance of every metric the cloud service collects via its own native API. WhatsUp Gold also monitors, alerts, and reports on interface traffic and bandwidth utilization by collecting network traffic flow records using Cisco NetFlow, NetFlow-Lite and NSEL, QUIC, Juniper J-Flow, sFlow, and IPFIX protocols. This allows administrators to optimize network performance, isolate network traffic anomalies and bottlenecks and establish bandwidth usage policies. WhatsUp Gold is used and trusted by tens of thousands of SMBs and enterprises all over the world. While regional requirements vary, the core ability to monitor networks and find and fix faults fast is in high demand everywhere. Ipswitch has WhatsUp Gold customers of all sizes on every continent but Antarctica.

Can you discuss what the market can expect from Ipswitch in 2019?

In 2018, Ipswitch had launched 18 new or upgraded products and this year will likely see even more. We are focused on delighting our customers with continual improvement in our MOVEit, WS_FTP and WhatsUp Gold product lines by introducing new features based upon both market requirements and customer feedback. Ipswitch is also continually expanding the breadth of products in line with our mission to make the networked world a safer place to share data. This will include new and expanded integration capabilities such as our MOVEit Mulesoft Connector. We intend to continue to develop software solutions for SMBs and enterprises that assure secure data sharing and high-performance infrastructures. Our efficient, easy-to-use products empower customers to respond faster to business demands through accelerated implementation and improved productivity. We anticipate delighting our loyal customers and developing new ones in 2019. ●



DR. MANOJ KARUNAKARAN

Senior Business Unit Manager,
Ingram Micro

A glimpse into the future

Dr. Manoj Karunakaran, Senior Business Unit Manager, Ingram Micro, paints a picture of the future and what partners must do today to optimize market developments.

If Artificial Intelligence (AI) is the future (present), ‘computer vision’ is going to be the most developing talk of the future. It is anticipated to be the biggest business in the next five years or so. It is a super ultra-modern technology, which is in the development stage but has accelerated recently and it is based on a computer video analysis in real time. The possibilities of this technology are infinite, and they are poised to reach with limitless boundaries. The market for computer vision is emerging as fast as AI to reach around \$20 plus billion by 2024. The expected entrance and consolidation to nowhere to all over within a glimpse must be watched with attention. Computer vision represents the capability of a machine to evaluate visual information and subsequently settle down on conclusions about it — where computer imaging can be used for controlling, automation, recognition and precise measuring. Developers are continuously exploring new

solutions that make use of computer vision and augmented reality. Product manufactures are

“**THERE IS NO LONGER A DEMAND FOR TRADITIONAL PARTNERS, WE NEED ‘NEW GENERATION RESELLERS’. WE ARE BUILDING OUR CENTER OF EXCELLENCE WITH ADVANCED AND FUTURISTIC SOLUTIONS FOR THE NEW GENERATION BUSINESSES FOR OUR RESELLERS TO BE IN LINE WITH THE NEW WAVE.”**

enhancing component execution and expanding cost efficiencies to improve this innovation to make it more accessible. As the innovation enhances, AI will figure out how to prepare AI, further streamlining the procedure and accelerating the rate of enhancement. The use-cases are unlimited with computer vision. Be it any modern circumstance, there is a possible computer vision-related solution that can be deployed. Global companies such as Amazon, Google, Microsoft including e-commerce sites have already started using image analysis in their predictive analytics efforts to forecast what their customers will want next time. In short, enhancing an image for a later use may be called image processing, while recognizing the objects and drive for automatic assessment and actions can be called as *computer vision*.

The revolution in the last few years are swift; partners will need to react and be ready to move ahead with the changes. Business models have changed with cloud, digital transformation, IoT, AI, Computer vision and

now we are all talking about the human and machine partnership, all these in shorter period. The biggest challenge is that channel partners need to act swiftly – quicker decision on investments, adequate training to their associates, quality resources who are willing to adapt with the pace – all are key for success. Nearly everything is moving to an OPEX model, end-user requirement is changing, the industry itself is changing that rapidly. There is no longer a demand for traditional partners, we need ‘New Generation Resellers’. We are building our center of excellence with advanced and futuristic solutions for the new generation businesses for our resellers to be in line with the new wave. Adaption is key. The quicker you understand the trend, the quicker you act on it. The faster you help transform the channel, the more likely you and your partners are to stay in business. This is a key priority for us and we are encouraging our partners to move in to the new solution selling model with human/machine blend complimenting it. ♦♦

STRUCTURED THINKING TO COMBAT CYBER CRIMINALS

Marc Kassis, Cyber Security Division Director, META, Ingram Micro on how end-users must adopt different solution thinking to combat cyber security adversaries.

Nowadays, IT security principles constantly change. All companies, organizations, governments and even private sector (SME and SMB) are discovering that a traditional security approach with even the most sophisticated technologies is not enough.

Traditional Cyber Security defenses are being circumvented by highly motivated criminals who understand the value of information from a successful breach. Criminals are highly skilled at what they do, and are becoming more sophisticated at exploiting systems, which can only undergo so much testing. Despite software vendors' efforts to combat this trend by hiring more testers and implementing tools to ensure created hardware or software is less vulnerable to hackers, it is not working. The cyber-attackers perfectly understand the IT world's most vulnerable area, this is: the human aspect, ourselves!

In this article, I will explore a few Cyber Security solution principles used in the market in 2019 to better protect assets. Including a modified mindset as to how investors, executives and IT users can save their businesses, data or intellectual property.

Traditional Approach:

When a new business venture is started, investors want to maximize their returns by establishing a company which has a lean organization with smart processes. To support such processes, smart, robust IT systems are required to seamlessly

and unobtrusively support the infrastructure and applications, which is scalable, fit for purpose and secure. However, with the big investment required to start a company, the need for Cyber Security approach to protect from threats to a business often come as an afterthought.

Start-up businesses are not alone in this consideration. Many well-established businesses are still coming across Cyber Security today with the same concerns. There is a need for education and the implementation of security technology.

In simple words, it is important to Protect. The size of a business determines the level of investment and the number of solutions to be implemented. Here is a snapshot of what is usually needed: Endpoint Security from vendors like Symantec, McAfee, Kaspersky Lab, Trend Micro, Sophos, Bitdefender, GFI, Carbon Black, etc. Firewall from some of the well-known vendors like Cisco, Palo Alto Networks, Forcepoint, Fortinet, Sophos, SonicWall, etc. VPN (Virtual Private Network) from few large Enterprise Infrastructure VPN vendors such as Cisco, Palo Alto Networks, Fortinet, etc. A much longer list of other vendor solutions is available for the private or Enterprise Software VPN. IPS (Intrusion Protection System) from providers like Cisco, IBM, McAfee, FireEye, Trend Micro, etc.

Now, depending on the maturity level of the IT and business, other solutions might be needed including: ATP, NGFW, NAC, WAF, DLP, Email

Security/Encryption, Web Security, PAM, DAM, IAM, CASB, etc. Companies using these solutions can be seen as following the Traditional Approach to Cyber Security.

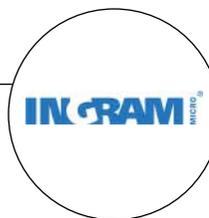
Enhanced Approach:

To secure the investment and understand how the security approach is effective, even once all the technology from a traditional approach is in place it can still be taken one step further. Reports or logs are required to understand how the invested Cyber Security solutions are protecting the network. This is achieved through the implementation of SIEM (Security Information & Event Management) whose role is to collect and aggregate information from all security devices and applications across the network. The outcome of a SIEM solution usually provides alerts with different levels of importance and severity. Attacks can be monitored in real-time for immediate and appropriate decision making, as well as plan for your upgrades or policy changes.

The major SIEM providers are IBM, McAfee, Micro Focus, AT&T Cyber Security (formerly Alien Vault), etc.

All solutions covered so far Protect a business, Detect and Stop attacks, next step is to Respond.

At this stage of security development, the Cyber Security technology strategy is quite active and can even be considered as very reactive with the implementation of the SIEM. Some major questions that come to mind here are: Is your Cyber Security



“**THERE ARE MANY THREAT INTELLIGENCE PROVIDERS ON THE MARKET BUT THE MOST EFFECTIVE ONES WITH THE FASTEST DETECTION OF MALICIOUS ACTIVITY ARE THOSE PUTTING ENOUGH RESOURCES AND SKILLS INTO THREAT HUNTING.**”

Marc Kassis, Ingram Micro META

strategy enough? Is it Proactive? Can you really anticipate the attacks? Are you aware of the current risk landscape on the internet? What is the worst attack that has happened recently, last week or yesterday?

This is what Threat Intelligence implementation can add to a Cyber Security strategy. Anticipate a possible threat.

The Cyber Threat Intelligence is a list of real-time feeds of information a SIEM will use to understand and interpret the threats that will or are currently happening or targeting businesses or organizations across the world. The SIEM will use it to prepare, prevent and identify among tons of collected logs all the threats directly concerned to a business. The hierarchy of the alerts and the accuracy of its priority coming from the SIEM is highly dependent on the Threat Intelligence feeds. This is also the way to reduce what is commonly known as “false positive”. The alerts which are classified as a threat or malicious activity, but while it is perfectly legitimate activity.

There are various Threat Intelligence providers on the market such as FireEye, Kaspersky Lab or Symantec. It is important to make an appropriate choice; therefore, I am sharing some of the most important elements to check with these providers.

Any business that follows the Cyber Security solutions already outlined, demonstrates a mature strategy in the form of a SOC (Security Operation Center) with several millions of USD having been invested. It is important to highlight that the SOC is not only a SIEM solution, but it is also a set of other tools, frameworks, resources and processes. It must operate 24/7 and have a certain level of comfort in reading the information to react quickly to alerts.

A mid-size organization or even an SMB need an Enhanced Security Approach and they can achieve the same level of features (Protection, Detection and Prevention) by choosing to buy the SOC as a Service from an MSSP (Managed Security Service

Provider). An MSSP will add several devices and applications to an existing security infrastructure to fulfil SLA obligations (Service Level Agreement). A commitment with an MSSP is typically for one to several years with payments on a monthly, quarterly or yearly basis.

Many Cyber Security vendors are having an MSS offering such as Symantec and IBM but there are a large number of independent MSSP on the market with several integrated solutions to offer the best SLA.

Going the Extra Mile – The Offensive Cyber Security:

While Threat Intelligence collects all information about existing threats and attack scenarios, it does not cover all malicious scenarios that are under development by cyber criminals. There are many Threat Intelligence providers on the market but the most effective ones with the fastest detection of malicious activity are those putting enough resources and skills into Threat Hunting.

Threat Hunting is becoming increasingly important in governments but also in large and modern corporations, as organizations strive to stay ahead of the latest threats. As a result, Threat Hunting becomes a must-have feature in any high-powered SOC. We are speaking about not only sophisticated tools but also highly skilled resources such as Ethical Hackers, teams of real-time developers as well as technology gurus. These resources are going to provide a fast path to extend Threat Hunting capabilities.

We then see the emergence of “Proactive Cyber Defense” or “Offensive Cyber Security”. It is defined as being the process of proactively and iteratively searching through networks to detect and isolate advanced threat activity. This implies that the Ethical Hackers must track cyber gangs and infiltrate them to understand their intentions before any cyber-attack scenario is even developed. Many reputable

Cyber Security vendors or MSSP offer a list of Threat Hunting activities to their clients which include “Social Media Sentiment Hunting”, “Enterprise Brand Surveillance” or even deep tailored hunting in the dark web for a given topic. In other words, finding the evil, hunting for adversary activity and eliminating the threat before it is developed

Threat Hunting and its detailed activity is the basic part of the new Advanced Managed Security Services. Commonly known in the market as “Managed Detection and Response” (MDR). It provides Threat Intelligence, automated Threat Hunting, Security Monitoring, Incident Analysis & Forensic and Incident Response. The major difference between the new MDR offering and the traditional MSSP offering is that the MDR goes beyond intrusion and malicious activity “Detection” but also “Responds” quickly to eliminate and mitigate the threat, with proactive hunting activities as described.

The MDR providers with Threat Hunting capabilities in the market today are just a small number even though many are claiming to be. Some of the large names such as IBM, Symantec, Cisco and FireEye are having a solid offering.

If you are looking to engage with one of the few MDR firms available on the market, remember to check the Threat Hunting activities they are offering within their packages. Most of them are claiming to only do automated Threat Hunting which is very similar to Threat Intelligence. Only a few are proposing the proactive and offensive activities.

This article touched upon the human element and how only people can stop other people’s motivation to harm or make money illegally through data theft. In my next article, I will be developing the human from the Risk Management aspect and how people can be the single point of failure inside organizations. Cyber Security is also the science of how to protect organizations’ business and values from insider threats. ●

Unlocking Cyber Security Potential



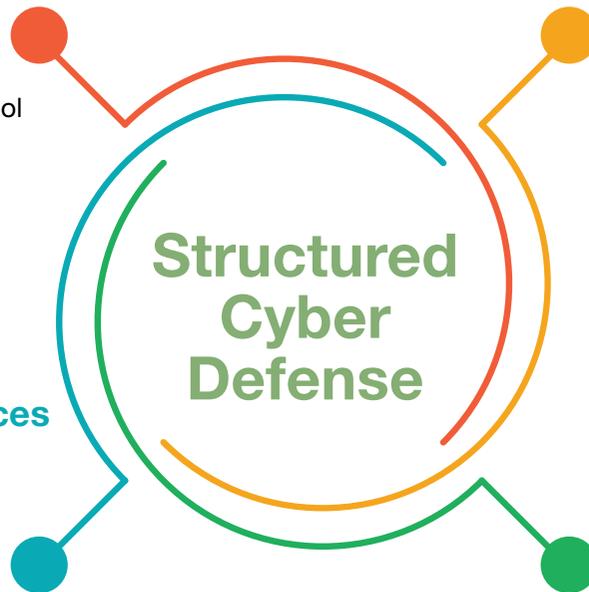
The Ingram Micro Cyber Security Center of Excellence offers an expansive suite of Technical, Consultancy, Managed Security Services and Trainings. We have also developed a wide range of Cyber Security services by building key and exclusive relationships with our vendors. As a result, we are able to help maximize our Business Partner's revenue potential and grow our vendors in the META Region.

Technical Assessments

- Public Discovery Report (PDR)
- Ingram Micro Self Assessment Tool
- Penetration Testing
- Vulnerability Assessment (VA)

Managed Security Services

- Digital Forensics
- Compliance Reviews
- Managed Perfection Response
- Threat Intelligence and Hosting



Consultancy Services

- Governance, Risk and Compliance
- Physical Classification
- Physical Security Assessment

Trainings

- Fundamentals of a Formal Information Security Risk Assessment
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Security Professional/Europe (CIPP/E)
- Certified Information Privacy Manager (CIPM)

Our META Cyber Security Partners



INGRAM MICRO CYBER SECURITY DIVISION

Web: www.cybersecurity.ingrammicro.com
Email: cyber.meta@ingrammicro.com

Tel: +971 4 369 7111
Fax: +971 4 369 7110

Address: Ingram Micro, P.O. Box 33550, Innovation Hub Bldg. 1, Dubai Internet City, UAE

BUILDING BUSINESS IN THE DIGITAL AGE

Micro Focus enlightens customers on how they can empower Micro Focus Data Protection strategy in the AI and IoT Era

In today's IT environments, customers' requirements have evolved to take advantage of the latest advances in technology to increase the power, flexibility and capabilities of the data center and remote offices. This is done to maximize the access and usability of the company data which is the core asset of any enterprise, large or small. The way data is stored, protected and handled has moved from a straightforward data center centric model to a hybrid IT schema. The new and diverse locations for data, together with the explosion in data volume create a growing problem about how to protect company data.

"Micro Focus Data Protector is an enterprise-class data protection application, delivering solutions for the most complex IT environments since nearly 30 years ago and that was added to Micro Focus portfolio after the acquisition of HPE software; a solution with a long history and a deep penetration into the market, which enables customers to centrally manage and orchestrate protection for data centers and remote offices.

It allows enterprises to reduce the cost and complexity of their backup operations while delivering improved reliability and business resiliency," said Jorge Dinarés, Sales President International (EMEA & LATAM), Micro Focus

It was designed to simplify and optimize backup and recovery for diverse, dynamic, and distributed environments, offering integrated automation, monitoring, and reporting—three tools businesses need to efficiently manage their entire backup environment from a single console.

Data Protector integrates with Micro Focus Operations Orchestration (OO), ITOM's enterprise-scale IT process automation solution that helps reduce operational costs and improve service quality by automating routine tasks, such as regular maintenance, provisioning of resources, and incident resolution. OO workflows automate routine backup tasks such as provisioning clients, managing and monitoring Data Protector services, running file system backups and restores, aborting active sessions, or adding and decommissioning virtual machines.



Jorge Dinarés, Sales President International (EMEA & LATAM), Micro Focus

“**IT ALLOWS ENTERPRISES TO REDUCE THE COST AND COMPLEXITY OF THEIR BACKUP OPERATIONS WHILE DELIVERING IMPROVED RELIABILITY AND BUSINESS RESILIENCY.”**



“**MICRO FOCUS DATA PROTECTOR IS AN ENTERPRISE-CLASS DATA PROTECTION APPLICATION, DELIVERING SOLUTIONS FOR THE MOST COMPLEX IT ENVIRONMENTS SINCE NEARLY 30 YEARS AGO.**”

Francisco Manzanero, Data Protection EMEA Sales Director, Micro Focus

Some of these processes take 15 minutes per client. With OO, they might take just seconds.

As commented, Data Protector offers powerful reporting capabilities out of the box, so users can enjoy the convenience of generating detailed reports from a single console, saving time and increasing productivity. Administrators can analyze and monitor their environments within the Data Protector GUI using a broad range of reports which allow them to view client backup statistics, sessions, backup schedules, storage pool and media usage, compliance, predictive and much more. These reports can be generated in a graphical chart and tabular view for a given timeframe. Administrators can interact with the graphical chart by selecting where more information is needed. They can also download the report, email it or add it as favorite to the Data Protector dashboard.

With regards Mission-Critical Applications, IT departments may be risking application outages by using backup software not designed to meet strict service level agreements (SLAs). This can occur when backup software is sufficient for basic tasks, but not for backing up systems that require 100 percent uptime, such as those used to record customer orders, billing applications, and payrolls. If the backup software does not use dedicated application integration agents, it can't ensure data consistency or support applications running in high availability mode.

A more effective way of protecting mission-critical applications is to use an enterprise-class backup and recovery solution that can scale extensively and integrate deeply with an organization's entire IT environment.

Micro Focus Data Protector uses this strategy.

It is a backup and recovery solution designed to work efficiently with critical applications such as Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server, Oracle Server, SAP HANA, IBM Db2, and MySQL. It does this by using backup APIs (such as SAP BackInt, Oracle RMAN, or Microsoft VSS) or file system agents for integrating with Windows, Linux, and Unix, including mission-critical HP-UX environments. It also interfaces with storage hardware from Hewlett Packard Enterprise (HPE), Dell EMC, NetApp, Hitachi, Oracle, and other vendors.

Data Protector protects mission-critical applications across hybrid IT environments. It integrates with VMware vSphere and Microsoft Hyper-V, eliminating the need for separate solutions for virtual environments. Companies can also use it to store data using public cloud services such as Microsoft Azure, and those from Amazon Web Services, and Ceph and Scalify storage systems.

The solution also integrates with leading cloud services to enable fast, seamless, and reliable backup and recovery in the cloud. It makes it simple for organizations to use cloud storage solutions as part of a single backup and recovery strategy.

Companies with multiple sites can also benefit from the solution. Rather than backing up data to tape and then sending it via courier to a remote archive location, Data Protector makes it easier to replicate backups across the network. Its federated deduplication capability works with systems, such as HPE StoreOnce Catalyst and Dell EMC Data Domain to transfer the data in a deduplicated state, reducing bandwidth requirements.

Based on above overview, “Micro Focus

decided to refocus our organization and develop a dedicated sales organization on Data Protector across EMEA. With this decision, and with the effort that has been made from the product development team, the results cannot be more satisfactory. In the last quarter, Data Protector has grown 50% in EMEA in the Backup & Recovery market, which grows 6%. This is mainly due to the improvements we have made in the last year in the solution and the fact that we have developed an organization dedicated to this product. This was an organizational decision that has yielded very good results. In fact, it is going to be replicated at worldwide level,” Dinarés said.

This approach allows Micro Focus to cover every region across EMEA and, aligned with the ITOM sales organization, deliver a value-added proposition to existing and new customers to provide a best-in-class solution for the new IT era. It also provides a clear message to the market about Data Protection Micro Focus strategy, that is supported by market analytics as in the OVUM report.

“Data Protector business has been a channel-driven business during the past years, with the announcement of a dedicated Data Protector team, and the new Micro Focus partner program, we demonstrate our continued commitment to provide an easier path for our partners as well as the resources and margins required by our partners to develop their skills and increase their share of wallet to confidently generate predictable revenue, build pipeline and do business with us,” said Francisco Manzanero, EMEA Data Protection Sales Director, Micro Focus. “We are looking for the best-in-class partners to work with them and develop a long-term strategy to achieve the expected targets”. ●



SAM JOHNY

Business Unit Manager,
Ingram Micro

The dirt has still not settled from the paradigm-shifting impact of Big Data on the way we work, largely due to technology continuing to coil upward at a confounding pace. With the Internet of Things (IoT) turning daily devices into a source of raw data for analytics to generate business insight, Artificial Intelligence (AI) is now coming of age to make analytics even more productive and efficient in the workplace. In the next year, organizations expect to have 20 to 2,000 times more data than today.

- **Data Application:** AI is changing both the competitive landscape and customer expectations to create a culture shift at top organizations. In the long run, this type of digital transformation improves the way we work. Leading organisations are experiencing a culture shift. This is championed by executives who realise that the digital transformation ushered in by

Leveraging AI in business

Sam Johnny, Business Unit Manager, Ingram Micro, explains how channel partners can help customers to integrate AI and security solutions successfully.

AI is changing the competitive landscape and shifting expectations. Customers are changing all aspects of how we operate. The biggest shift is how we view, value and monetize information - made possible through data-driven decision-making.

- **Analytics Drive Innovation:** Trends have changed customer expectations that drive the need for data-driven insights - often in real-time. The development of streaming

analytics, edge analytics and other innovations have made it possible for organizations to meet those expectations, enabling a responsiveness that ranges from providing optimal customer experiences.

- **Intelligent Machine and Pattern Recognition:** AI capabilities can be anything from implementing image recognition to analyzing consumer spending behavior for fraud. Even the smallest changes to achieve more focused insight into trends and patterns allow powerful AI capabilities to yield big results from complex data sets.

to enable faster decision-making and free up valuable resources for stakeholders. AI has the potential to provide a wealth of insights that both confirm and dispute previously assumed hypotheses. Combined with human expertise, this augmented intelligence will help businesses drive cost savings, increase talent quality and improve the effectiveness of their contingent workforce programs.

An increasing amount of data processing isn't the only area of opportunity, information security plays a huge role in building a strong AI platform. Channel Partners play a huge role in building AI and Security at a scale and at a pace that is required currently for the Total Addressable Market. Those partner who adopt this paradigm shift quickly will be able to transform better and play a key role in transforming their customer to be ready for the future. End-customers always trusted channel partners to come with new solutions that can reduce operations cost and increase efficiency. The adoption of machine learning, and other AI technologies provides new insights into a wide range of aspects and new ideas will help the organization to move far ahead. ●

“**CHANNEL PARTNERS PLAY A HUGE ROLE IN BUILDING AI AND SECURITY AT A SCALE AND AT A PACE THAT IS REQUIRED CURRENTLY FOR THE TOTAL ADDRESSABLE MARKET.**”

Successful businesses understand their target customers and build business models around them. Those who want to better understand customers can benefit from the new opportunities afforded by artificial intelligence—but only if human insight informs machine learning and improves algorithms. The increased integration of AI into existing technologies is poised to unlock a wealth of opportunities for businesses. By analyzing data sets and performing automated work behind the scenes, AI promises

IP Surveillance and Security Solutions

 <p>IP Cameras</p>	 <p>Video Storage Solutions</p>	 <p>Specialized Solutions</p>	 <p>NVRs</p>	 <p>Accessories</p>	 <p>Access Control</p>
 <p>Perimeter Protection</p>	 <p>Video Analytics Software</p>	 <p>VMS</p>	 <p>Professional Services</p>	 <p>Infrastructure & Connectivity</p>	

Access to technology from best-in-class security brands



BASSEL AL FAKIR
Managing Director of NIT

Video Surveillance Data in the AI and IoT era

Surveillance video is more than just a video – it’s precious evidence for an incident, and it is growing faster than ever, says Bassel Al Fakir, Managing Director at NIT, an Ingram Micro Company.

Artificial intelligence (AI) is a game-changer in the Surveillance industry, machine or deep-learning is widely used for video analytics today. Artificial Intelligence systems able to analyze vast amounts of video data and “learn” how an object looks, how fast or in what direction it moves, is it human and recognize its face, gender, age group, etc. It can also recognize objects, like mobile, an umbrella or vehicle license plate or vehicle model. AI can roughly define an incident and then alert a human being, who then decides the response creating a new level of intelligent security.

Internet of Things (IoT) - connected “smart” devices that interact with each other and us, is exploding from 2 billion devices in 2006 to a projected 200 billion by 2020, and so the amount of data produced grows exponentially. The IoT ensures connecting everything

from CCTV cameras, medical devices, smart home products, smart enabled vehicles, and many more devices. Companies are looking for a solution that can bring together collected data, store, secure and manage this data in the most sophisticated way.

The storage of video recordings and how to ensure that they are retrievable and fit for purpose are the most critical components of a surveillance data. The sophisticated and intelligent enterprise-grade Surveillance solutions require functions such as real-time access to recordings, and instant alerts to extraordinary events need to have storage systems that meet the

highest demands.

How to reduce the Storage? The cloud data centers and edge computing, when data processing kept within the camera itself or technologies like Zipstream, the intelligent video compression method can significantly reduce the bandwidth and storage demands of both data transfer and storage and work in balance together.

There is a multitude of storage solutions out there. Before you buy one, it is crucial to understand: What is the nature of the surveillance system? What is the scale of the data output? How and why data will need to be retrieved? What type of cameras is in use and how many?

“THE SOPHISTICATED AND INTELLIGENT ENTERPRISE-GRADE SURVEILLANCE SOLUTIONS REQUIRE FUNCTIONS SUCH AS REAL-TIME ACCESS TO RECORDINGS, AND INSTANT ALERTS TO EXTRAORDINARY EVENTS NEED TO HAVE STORAGE SYSTEMS THAT MEET THE HIGHEST DEMANDS.”

Is the number of cameras likely to increase? What is the purpose of recorded video? What is the camera resolution?

In NIT an Ingram Micro Company we work with one of the best infrastructure providers in the world, helping our Customers to build robust end-to-end surveillance platforms that are open, scalable, and ready for management of their disparate data sources. ●





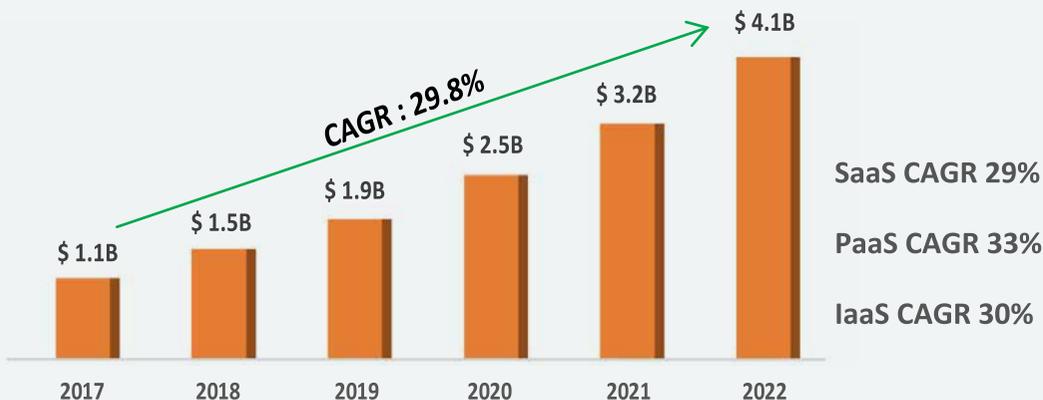
BUILDING A PROFITABLE CLOUD BUSINESS WITH INGRAM MICRO

Guruprit Ahuja, Director Cloud, META at Ingram Micro, shares his thoughts on how to build a successful cloud business practice & the opportunity for cloud business in the META region.

META MARKET INSIGHTS

According to the latest IDC reports, the worldwide public cloud spend on cloud services and infrastructure is forecasted to reach \$210 billion in 2019, an increase of 23.8% over 2018.

META Public Cloud Spend



WHAT TO EXPECT IN THE NEXT FEW YEARS?

- Opex shift** - IT operations will be succeeded by AI-driven automation resulting in significant Opex savings.
- Need for cloud services** - Demand for public cloud SIs and brokers will rise.
- Skillsets** - Automation will drive the need for skills around business process redesign & industry expertise.
- Digital workers** - Employees will access AI-infused software to prepare themselves to become "digital workers".
- Rise of Automation** - Enterprises will look to automate everyday repeatable tasks.



THE GOOD NEWS IS THAT WE UNDERSTAND OUR CHANNEL ECOSYSTEM IS NOT AS MATURED AS IN SOME OF THE DEVELOPED MARKETS WORLDWIDE."

OPPORTUNITY WITH XAAS

SaaS - As enterprises look to go Opex, the biggest volume and run-rate opportunity lies with SaaS business. There are several vertical & horizontal solutions to capitalize on most of which complement the existing business practices.

IaaS & PaaS - For beginners, the ideal approach to IaaS business will be through key workload selling such as Backup, DR, Test & Dev, Capacity expansion along with associated implementation, migration & managed support services. The real opportunity with IaaS & PaaS along with highly profitable services will be with business transforming workloads such as Lift & Shift, DevOps, IoT, etc. These workloads compliment use cases which directly improves a company's operational efficiency & productivity. At the same time, they change the way companies address and offer an experience to their customers.

Managed Services - Customers are increasingly becoming self-aware and their need to automate & innovate, go-to-market faster than competition requires adoption of the modern-day XaaS solutions. As more customers look to deploy multi-cloud & complex hybrid-cloud environments, the need for managed services & cloud orchestration represents the biggest opportunity for the channel ecosystem.

HOW TO BUILD A SUCCESSFUL CLOUD PRACTICE?

Create your differentiation

Increased competition and commoditization of SaaS & IaaS solutions implies that the channel ecosystem needs to create a differentiation to beat competition. Reselling a few software licenses is no longer a sustainable business practice.

Attach, Upsell, Cross-sell - If you have a set of customers you have sold an email service to, you can attach, upsell & cross-sell several

solutions which complement the email service. Broadly, these solutions fall in the categories of migration, backup, mobile device management, archiving, security, digital transformation, unified communications, etc.

Broadly, these solutions fall in the categories of migration, backup, mobile device management, archiving, security, digital transformation, unified communications, etc.

Sales approach - In order to be successful, your sales approach needs to be pro-active. Apart from being able to address pain areas of your customers, your sales teams should be equipped with the knowledge to create a need for upsell & cross-sell solutions. Besides, your sales teams need to be incentivized and goaled on selling cloud solutions. This will help build the foundation of the recurring cloud business model for the years to come.

Customer experience - You need to leverage automation for delivering solutions and services faster to your customers. Your customers are used to buying digitally via ecommerce platforms in their personal lives. Business solutions delivered via leading hyperscale cloud platforms such as CloudBlue help improve your customer buying experience.

Modern-Day Marketing - The legacy ways of marketing such as email marketing is no longer enough to generate customer demand. The approach to marketing has transformed with new innovative, analytical, video-led and programmatic marketing solutions. As a company, you need to invest time and resources in building efficient modern-day marketing practices to facilitate demand generation from your customers and prospects.

Assess

In order to build a successful cloud practice, you need to assess the following:

- Your business goals

- Your customer & prospect segmentation
- Your sales and technical readiness

Plan

- Cloud GTM strategy
- Your solutions portfolio
- Sales & Technical enablement
- Demand generation
- Investments & resources

Execute

Once you have created a differentiation, assessed your business goals & planned your GTM, an effective execution of the GTM plan is needed. ●

HOW INGRAM MICRO CAN HELP?

The good news is that we understand our channel ecosystem is not as matured as in some of the developed markets worldwide. We at Ingram Micro want to help you build a successful cloud business practice.

Book a business consulting workshop with us today to

- Assess your business goals
- Create a differentiation for your business
- Transform your sales approach
- Enhance your customer experience
- Implement modern-day marketing methods
- Plan an effective cloud GTM strategy

sales@ingrammicrocloud.me

Ingram Micro IaaS Solutions & Services Portfolio



BCDR

Protect your data using cloud backup & DR solutions



Test & Dev.

Spin up servers for testing and dev. in minutes



Capacity Expansion

Expand your IT infrastructure on demand with cloud



VDI

Deliver applications and virtual desktops from cloud



Hybrid Cloud

Integrate cloud with your existing IT infrastructure



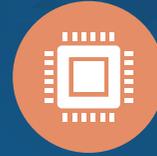
Lift & Shift

Migrate fast to cloud without re-architecting your apps



DevOps

Use cloud to deliver software faster & more reliable



IoT

Connect & analyze data received from IoT sensors on cloud

Ingram Micro Services

Pre-sales

Business Transformation Consulting

Cloud readiness assessment

Deployment planning workshop

ROI / TCO calculation

Solution architecture & design

Post-sales

Implementation / Migration Services

Managed Services:

- Updates & patch management
- IaaS / Application monitoring
- Security monitoring
- Cost optimization
- Support – Email, Chat, Phone & On-site



JULIE VARGHESE

Business Unit Manager,
Ingram Micro

Regional customers are currently leveraging major solution offerings from Big Data and analytics vendors. At Ingram Micro, we have offered solutions to many government and financial institutions across the Middle East region.

Many organizations are still in the Descriptive stage when it comes to data analytics, utilizing traditional BI approaches, which includes getting all data together and using visualization to gain quick views on what has happened. During the Diagnostic analytics stage, it's all about figuring out why an incident took place, and using techniques such as drill-down, data discovery, data mining, and correlations. Most analytics frameworks have been incorporating such features in their offerings. However, where it gets interesting is when trying to use predictive analytics to project what will happen. Typically, this is done by using existing data to train predictive machine learning (ML) models and this is why analytics is part of the evolution that leads to AI.

Successful AI-enablement requires more than just a technology strategy;

Embracing AI

Julie Varghese, Business Unit Manager, Ingram Micro, discusses how customers can embark on the path to transforming their operations from Big Data to AI.

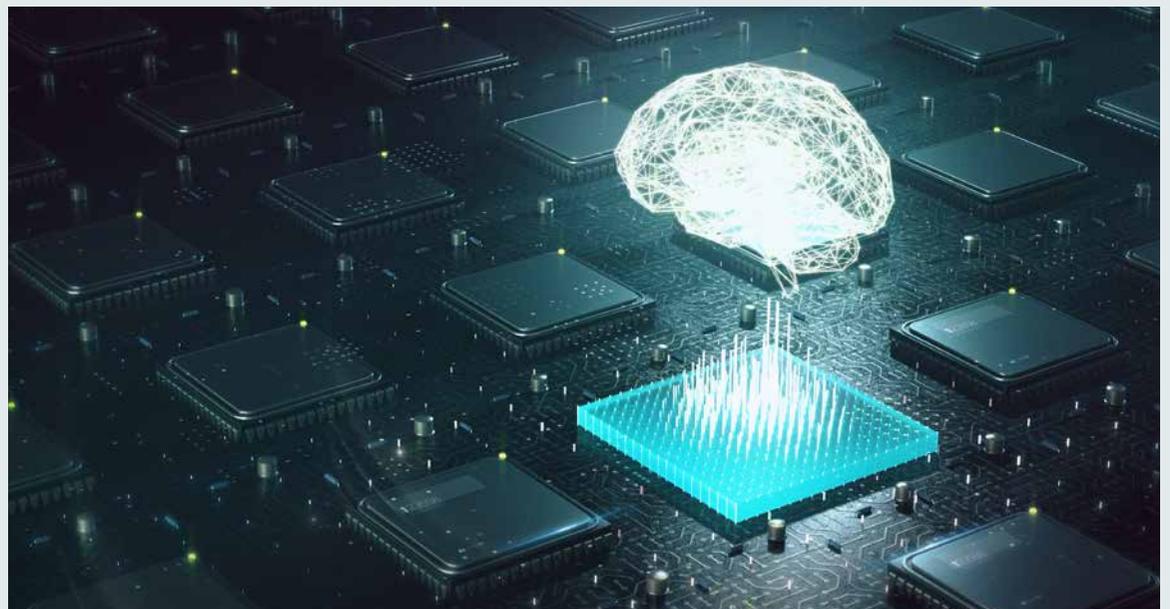
it requires the transformation of an organization's people, processes and technology. At Ingram Micro, we follow a three-step approach - Ready, Build and Go-To-Market (GTM). The first approach involves aiming at educating the channel on AI and the transformation it can bring to the business. In the 'Build' stage, we are focusing on consulting, building solutions with vendors and

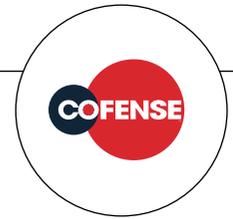
partners, helping the channel with deployments and so on. The third approach, which is GTM consists of many activities such as events, webinars, demand generation activities, lead qualification and so on.

We are also investing in skilled resources, i.e. data architects, data scientists and AI developers.

As AI begins to deliver results and draw interest from all areas of the

business, it introduces a host of new requirements and challenges. AI is changing the way we develop products, the pace we develop products, and the way our products go to market. As with most digital transformation endeavors, achieving successful AI-enablement goes beyond just a technology strategy; it really comes down to transforming people, processes and technology. ●





THE UNCOMFORTABLE TRUTHS ABOUT PHISHING

Pat Dunne, Senior Channels Director, Europe, Cofense, educates regional customers and partners on how to thwart phishing threats effectively.

What aspects of the conventional phishing approaches do customers need to move away from?

Companies tend to focus on simulation and training as an awareness solution, with the goal to drive down user-clicks on suspicious emails. The reality is it's impossible to get to zero clicks on phishing attacks. Our statistics show that with simulations of similar sophistication to phishing attacks hitting companies today, our customers average over 11% click (failure) rate. Companies with this mindset therefore remain vulnerable and sometimes worse, complacent. The focus is on getting users to report suspicious emails to give visibility to an organisation that they are under attack.

Can you briefly explain the uncomfortable truths about phishing?

An Uncomfortable Truth is something that challenges, or contradicts traditional, or conventional thinking. Rather than focusing on theoretical risks, organisations must accept that real phish are the real problem. By that we mean that security teams must focus on how they will maximise their visibility of phishing threats, and then deal with them. For example, the first uncomfortable truth of phishing defence is that no matter how good your perimeter controls, malicious emails are still reaching the inbox, and it's a common misconception that users are the problem, as they are the ones who click, potentially causing compromise or breach. However, users who are well conditioned to recognise evolving phishing threats, and are enabled and empowered to report suspicious emails, act as valuable human sensors to provide



Pat Dunne, Senior Channels Director, Europe, Cofense

visibility of threats that technology has failed to prevent. However, most organisations are unable to effectively respond to phishing attacks. The reasons for this vary, but are typically related to lack of time, or lack of experience or exposure to the latest threat actor tactics and techniques. To turn the reports of suspicious emails from users into actionable intelligence, security teams must be able to prioritise, analyse and understand what has been reported to enable effective threat mitigation actions, such as quickly hunting for identified threats across the email environment, and timely quarantine to minimise exposure.

How can customers move away from traditional approaches to be more effective against phishing?

Phish 'testing' is the enemy of effective phishing defence. Users must recognise the role they play in protecting the organisation and its data. Engaging the users to report suspicious emails, both simulations and real, then communication

positively with those that report real phishing creates an atmosphere of collective defence.

How is Cofense enabling customers and partners to thwart these threats head on?

Cofense builds a culture of reporting suspicious emails, then provides tools to quickly identify which reported emails are really phishes. This allows the company to stop those attacks within hours or even minutes of them arriving in the user's inbox. We also provide the ability to find unreported emails for other users from the same or similar attacks and remove them from the user's inbox.

Many companies either don't have the time, resources and skills to implement these strategies, but need them up and running fast. For the last 3 years we've run a managed service offering to help our largest customers implement these strategies. More recently we developed a managed service offering for partners who want to add phishing defence to their managed security services offerings to their customers.

How does Ingram Micro play a role in your growth strategy?

As well as everything you'd expect from Ingram in terms of partner access, logistics, training, etc. Ingram are planning a managed service around our products. This means resellers can offer their customer a fully managed phishing defence solution as a service enabling customers to address this issue without being distracted from their core focus.

Can you elaborate on your market plans for 2019?

We have a strong presence in the region and already have a large and well-established customer base. We are looking to build on this through a limited number of focused cyber security resellers, who can bring our message to their customers. We will also develop a limited number of MSSPs. We have sales and technical resources in region to assist these partners and have programmes to drive marketing campaigns, training and certification. Our partner programme allows for deal registration enabling us to work with proactive partners on opportunities with good margin. ●

INGRAM MICRO[®]



The Future is Here.

New Office,
New Experiences.

 2nd Floor, Building 1, Innovation Hub,
Dubai Internet City - UAE P.O. Box 33550

 +971 4 369 7111  ae.ingrammicro.com

SOLUTIONS

Accelerating Digital Transformation

Ingram Micro, the world's largest IT distributor, offers a wide range of added value technology solutions to channel partners and businesses of various sizes. Under the Solutions brand, Ingram Micro aims to help the IT community in Middle East, Turkey and Africa region to accelerate their digital transformation journey.



AI and IoT



Augmented Reality



Cloud Technology



Connected Vehicles



Cyber Security



Data Capture



Data Centers



Digital Singages



Drones Technology



Enterprise Network



Enterprise Software



Physical Security

Join Ingram Solutions journey to explore a limitless world of opportunities and keep realizing the promise of technology.