Digitaltech Media
Inform, Inspire, Innovate!
▪ Vol I Issue 3 ▪ September 2020

VAD
How VADs Help Complete the ICT Ecosystem?

UAE MARKETSCAPE
UAE gearing up to the need to Secure the Cloud

TRENDING
Rethinking Cloud Security Strategy Amidst Pandemic and Mounting Threats

CXO TALK

Harmit Malhotra on his stint at Republic Media Network

Digitaltech Media
Inform, Inspire, Innovate!

How VADs Help Complete the ICT Ecosystem?

Despite the growing trend towards transparent or pure models of distribution, the VADs or the Value-added distributors of the ICT industry will continue to hold a relevant position in the supply chain. Why?

Well, the value-added distributors have an extensive understanding of customer needs, industry trends, how the market forces come into play, as well as the technical resources required for backing their position. Together with the vendor and the resellers, the VADs help to form strong relationships that further enables each one of them to strike favourable deals.

VADs Adding Value in the ICT Space

Over the years, VADs have managed to form meaningful, as well as mutually productive relationships with the value-added resellers, thus securing their place in the ICT supply chain. VADs have excelled in areas such as consumer products like laptop and PC distribution, printers & peripherals, software products, and even other segments such as wireless implementations, LAN/WAN networking, disaster recovery, SAN, and disaster recovery among others.

RAJESH GOENKA,
Director, Sales & Marketing,
RP tech India

"The IT channel business cannot be complete without vendors, value-added distributors, and channel partners. Each of these three stakeholders has

DEBRAJ DAM,
Chief of VAD, Supertron India

different expertise, strengths, and capabilities, and all of them require support to grow," said Rajesh Goenka, Director, Sales & Marketing, RP tech India.

As one of the leading value-added distributors, RP tech India offers pre-sales expertise, order execution at multiple locations, and post-sales support to partners to ensure a win-win situation for all. Apart from this, the VAD also offers financial capabilities to execute large projects.

Kolkata based Supertron, on the other hand, offers a combination of inventory & logistics expertise

BAIG FIROZ,
National Manager - Technical, Satcom Infotech Pvt. Ltd.

alongside training, and the right mix of OEM products that further helps them to meet customer needs, and deliver appropriate solutions.

"We help partners to reduce response time to their customers by acting as the bridge between OEM, partners, and end consumers. We offer value-added packages from our product offerings, and solution scope as well as aid the partners through our four support pillars including, Product Specialist, Sales, Solution Advisor, and Post-sales," stated Debraj Dam, Chief of VAD, Supertronindia.

Adding Value without the Product Becoming Overpriced

One of the first things that VADs do is that they help the resellers or the dealers to build the confidence required for better promoting the product.

"Instead of investing in their team, dealers can collaborate with VADs and take advantage of our ability to promote the product. This will eventually help the reseller partners or the dealers to grow their business with less investment aside to striking profitable deals," stated BaigFiroz, National Manager - Technical, Satcom Infotech Pvt. Ltd.

Goenka of RP Tech believes that every VAD is expected to offer value-addition in the form of pre-sales, post-sales, and digital marketing. "Each of these can be explored without incurring an enormous cost," he reiterated.

Challenges Galore

Given the pandemic and economic downturn, questions are being raised around financial stability, as well as the viability of the organizations that offer value-added services. As a result, VADs are facing multiple challenges such as reaching out to the end customers individually amidst the WFH (Work from Home) culture. Apart from this, there are other challenges, like lack of planning and availability of infrastructure to tackle such situations.

"We have been working hard to gain partner and end-customer trust. As a VAD, I feel we function as an extended arm for both the partner and the OEMs. Given the current COVID-19 circumstances, we have started charging on behalf of the partners to maintain complete stability and to offer the best services," reiterated Firoz.

Supertron also acknowledges the fact that the existing scenario needs to be viewed as an opportunity to collaborate with the partners in an organized manner.

"We have witnessed a bounce-back of the enterprise segment after the April set back. Our team has managed to build a good funnel together with SI and OEM's. Although we are witnessing some challenge, as far as payments are concerned, we have managed to solve these issues through a webinar. We are also looking to reduce the multi-vendor contact point for future business growth" said Debraj.

Echoing similar sentiments, Goenka of RP Tech mentioned that they too witnessed few hiccups on their way to ensuring business continuity during and post the lockdown period. While the nation-wide lockdown put constraints in the movement of goods and affected the VAD's overall business growth, they also witnessed financial strains due to limited business prospects and bank credits in the last few months.

But, the distributor focused on employing their over two decades of experience, and strong relationship with channel partners to find a way forward. "For us, the value addition business has emerged strongly since August, and this trend will continue for the next coming months. We believe that most of the VADs have seen an increase in their business, and we now see no challenge in terms of business continuity and long term sustainability," shared Goenka.

What Differentiates the VAD in the Ecosystem?

Going forward, the biggest differentiator for the VADs within the ecosystem will be their ability to reduce the multipoint product contact window, which would eventually make it easier for both the partner and its customers to coordinate with each other.

"The ability to deploy these services on a broad scale is increasingly a differentiator for the VADs. If the reseller cannot support the skills needed to perform all or some of these tasks, other members of the supply chain must deliver them. It is here that the strength of the partnerships will be tested," stated Firoz.

Sharing similar views, Goenka reiterated, "Pre-sales, post-sales, and strong logistical support will be the major differentiators for the VAD in the entire supply chain."

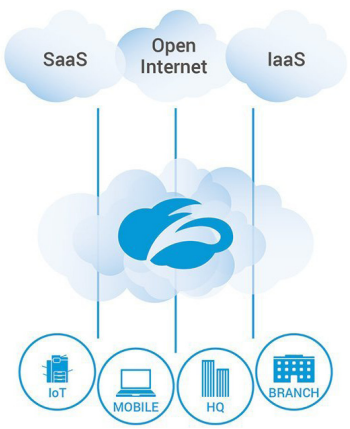
Conclusion

To sum up, while some people have been arguing the very role of VADs in the distribution channel, and that their position will be taken over by the vendors and the reseller partners sooner or later, the fact remains that both stand to benefit tremendously by partnering with the VADs.

PRODUCT REVIEW

ZSCALER WEB SECURITY REVIEW

Zscaler Web Security is a safe web passage conveyed as a cloud administration, intending to give organizations the insurance they require to shield themselves from online dangers. The Zscaler stage safeguards against malware, progressed dangers, phishing, program misuses, pernicious URLs, and botnets. Just as web security, the administration offers web separating, firewalls, and against spam capacities. Administrators approach constant revealing and incorporated investigation to guarantee all clients are sheltered from dangers. Zscaler was one of the primary organizations to offer cloud web security which worked with negligible programming introduced on a client's work area.



Features

- Cloud Sandboxing for protection against malicious files.
- DNS Security to enable protection against viruses.
- Analytics and time logs for visibility and progress.
- Administrative Controls to include filtering of bandwidth, URL, and DNS.
- Data Protection against threats.
- Smart Cloud Assistance, including SSL visibility.
- Reduced Latency to provide a super-fast scanning.
- Office-365 Integration is available at a click.

Review

Zscaler is a market driving cloud web separating choice for medium to enormous estimated associations searching for solid web security with approaches to shield clients from online dangers and screen how representatives are utilizing the web. There are granular administrator controls on offer to channel explicit site pages and ensure that web sifting is fit to various groups inside the association. This stage is completely cloud-based. Thus, the arrangement is simple, with security for all clients, in any event, when off the work organization. The stage has solid execution, with low inertness. There is a scope of reports and reviews just as constant permeability over how individuals utilize the web. Notwithstanding, there are likewise some helpful end-client controls, for example, a 'proceed in any case' include, which permits individuals to visit destinations they know to be sheltered, in any event, when Zscaler recommends they don't. This can be a decent method to permit workers to be secured, without antagonistically affecting their capacity to carry out their responsibility. Organizations searching for solid danger assurance with administrator controls ought to think about the Zscaler stage.

HARMIT MALHOTRA WEAVES HIS SUCCESS STORY IN THE IT BROADCASTING SPACE

The journey of Harmit Singh Malhotra, who is the GM-IT (Broadcast & Corporate)at Republic Media Network, in the media space has been nothing less than fascinating. In his 20 years of experience, he has had the opportunity to explore not only IT corporate and Broadcast but he could also enhance his skills that gave him the exposure in both the fields.

HARMIT SINGH MALHOTRA,

GM-IT (Broadcast & Corporate) – Republic Media Network

Over the years Harmit got the chance to work with big Media houses like TV18 Broadcast, STAR India and Republic Media network and this is where he explored avenues like IT Corporate, Broadcast, Cyber Security and Digital respectively. From setting up the studios and uplinking operations of Republic TV to launching of Rbharat in a span of just 4 months, Harmit has managed these responsibilities in his capacity at Republic Media Network.

Having built a dynamic career with innovative problem solving and great team building skills, Harmit admits that he loves to experiment with new ideas while taking up challenging roles in the interest of his organization.

However, his stint in the IT broadcasting space was not without challenges. While trying to carve a niche in the broadcast media industry, one of the major challenges that Harmit had to face was to change the perspective of the decision makers from traditional working to modernisation of the technology while also introducing automation in day to day working. But this did not deter him in following his dream. In fact, his faith in Almighty and his determination to work towards his goal kept

"I started my career with TV18 Broadcast, where I equipped myself on IT broadcasting. IT broadcasting has a wide horizon and with passage of time I started exploring the various avenues of this field," explains Harmit"

him on his feet all the time and this he proudly states is his success mantra in building the brand 'Harmit'.

Digital Transformation - the new buzzword

Digital Transformation is the latest buzzword for every CIO today in terms of delivering value to customers as well as spearheading the organization to success. "It is a hard fact that Digital is now indispensable part of every organization," says Harmit."However the biggest challenge with any organization is choosing the correct module as per its requirements."

Moreover, Harmit is of the opinion that the role of a CIO has transformed from that of passive to active with them working on the front row now while managing the organization requirements. "This is an era when technology evolution is at its peak and is having a major impact on the business. Seeing the current scenario I feel CIOs should be more open and accepting towards change," he opines.

While talking about technology evolution Harmit also pointed out the coming of the new media – the social media, OTT platforms as a modern means of content consumption. "With the advent of the new age digital media, OTT platforms are like the extended hands of any media house," he says. "OTT consumption has increased as much as 200% and is by and large accessed by all age groups across the globe. Keeping in pace with the current scenario as a CIO I feel that OTT is now an integral part as smart phones are easily accessible and low cost internet packages has made it reach far and wide. Since OTT is still evolving it offers a lot of scope for innovations and optimizing the same is what CIOs are now focussing on."

Leaving aside his professional life, when asked what does he love doing most in his pastime, Harmit says that he enjoys cooking as it is like a stress buster for him. He also loves playing with his 6 years old daughter and travelling to new destinations.

Rethinking Cloud Security Strategy Amidst Pandemic and Mounting Threats

Cloud security is not a new concept, but it certainly is one of the most critical components of the cloud environment. As cybercriminals continue to search for loopholes to exploit the security infrastructure, it is crucial to implement robust, dynamic, agile, and effective cloud security solutions, similar to the cloud computing infrastructure that needs protection. An effective security system must protect connections between users and data, apart from securing all the other connections to every virtual or physical device that forms a part of the infrastructure.

Often, this results in numerous complexities since the deployment of security solutions may differ from one cloud platform to another, and can also have their functional limitations. It is this kind of deployment that limits the actual potential of cloud computing, and many organizations fail to address the security challenges holistically.

Before the COVID-19 disease hit the world, the cloud security adoption rate was growing at a steady pace. In 2019, cloud computing witnessed a steady rise from 24% to around 86% over six years. COVID-19, however, caused this adoption rate to spike further, in particular, because of the growing need to work remotely. Cloud-based virtual desktop infrastructure and other collaborative tools help employees to stay in touch with one another. It has further increased the confidence of enterprises who have or are in the process of embracing cloud computing. As the novel coronavirus continues to spread further, business leaders and executives have come to realize that cloud security is the key to building resilient organizations in the future.

Cloud Security

TRENDING STORY

Cloud Security-The Prime Concern for Organizations

A report released by Research and Market revealed that the Indian cloud infrastructure market is estimated to expand at a CAGR of 23.61% during 2019-2024, and will likely reach a value of INR 196.46 Bn by 2024. There has been a massive increase in the cloud adoption rate during the pandemic, especially in the wake of the Digital India movement, launched by the government. However, the rise in the adoption of cloud technology also brings along with it an exponential increase in cybercrimes.

According to the SonicWall Capture Labs that released their cyber threat report for mid-year 2020 recently, there have been massive increases in the ransomware, IoT malware attacks, and opportunistic use of the COVID-19 pandemic.

The report analyzed threat intelligence data gathered from 1.1 million sensors in over 215 countries and territories. Thus, the labs recorded a 50% rise of IoT malware attacks, 7% of phishing attacks

DEBASISH MUKHERJEE,
VP -Regional Sales, APAC at SonicWall

that capitalized on the COVID-19 pandemic, and a 176% increase in malicious Microsoft Office file types.

Given the above scenario, there is no arguing the fact that cloud security has become one of the prime concerns for both the enterprises and the cloud storage providers at the moment.

The current norm of remote working has forced industries to migrate to the cloud to support their businesses from their homes. Those that continue to rely on the traditional methods will fail to survive unless they adopt the latest technologies. Remember, users today access all their files without having to keep the bulk of that system on their computers. People use cloud computing services, such as google drive, Instagram, Facebook, Gmail daily. Besides, the consumption of OTT platforms has also increased multifold.

Given the above increase in security breaches, enterprises are either disabling their application or websites or losing a significant amount of their annual turnover. Hence, cybersecurity has gained prominence among cloud storage providers.

"COVID-19 led pandemic has introduced a new order in society and has acted as a catalyst in terms of speeding up the overall process of adopting cloud security globally. The need to work remotely supercharged the adoption rate of cloud security," says Debasish Mukherjee, VP, Regional Sales - APAC at SonicWall.

He further explains that as enterprises have moved to work from home culture, their devices have now become truly limitless. Employees continue to use their devices, including their mobile phones, or even the iPads, and their corporate laptops. Children are also accessing their parent's laptops to do their school work that further opens up a multitude of vectors that a lot of people fail to take into consideration. Given the above scenario, cloud security has indeed become the need of the hour for all the cloud storage providers to adopt.

Echoing similar sentiments, Adam Palmer, Chief Cybersecurity Strategist, Tenable opines that the perception that the cloud is more vulnerable than on-premises technologies is false.

Thus, it does not matter where the infrastructure or applications reside, because if they are connected, they are potentially vulnerable. Organizational heads need to understand this and implement cybersecurity strategies that address new and emerging threats.

"Stay-at-home orders pushed many organizations to leverage new cloud-based technologies and approaches to optimize their performance. But, as with any new technology, it expands the attack surface, and there have been reports of cybercriminals targeting users in a variety of ways, including leveraging malicious emails to phish users and spread digital viruses. Organizations will have to rethink business models that align with new working patterns, customer demand, and supply arrangements. Security teams will have to re-establish effective controls over a new hybrid home and office working model," Palmer reiterated.

How Can Cloud Security Help Despite the Evolving Threat Landscape?

ADAM PALMER,
Chief Cybersecurity Strategist, Tenable

Typically, when companies migrate to the cloud, they focus primarily on the cloud infrastructure, rather than cloud security, which is often an afterthought for them. Given the existing threat landscape, different layers within the cloud need safeguarding. In other words, it is crucial to protect email, data, and user credentials from advanced threats while ensuring compliance in the cloud.

"Cloud is useful for businesses due to its flexibility and remote access, which is attractive in today's business environment. It is useful but is not risk-free and is critical to the sustainability of the business. With hackers getting creative and more aggressive with their techniques, they can take advantage of a slight breach and steal sensitive information and data," says Mukherjee.

Thus, cloud security needs to be prioritized by all the organizations moving to the cloud to protect them against the spike in the number of phishing attacks through malicious links and apps that hack devices, as well as steal user data. As far as cloud security is concerned, it offers many benefits, such as visibility, next-gen email security, advanced threat protection, data security, and compliance.

Palmer, on the other hand, believes that while the threat landscape has evolved, security solutions failed to keep up, creating a massive gap in the ability of the organization to understand their cyber exposure.

"Cyber exposure gap has left organizations vulnerable and exposed. Enterprises need to think strategically about their security programs, ensuring that they are investing in the right solutions and tools to tackle modern IT challenges. The right security solutions can help security teams eliminate blindspots and gain unparalleled visibility into the security status of their modern IT infrastructure," he added.

Managing and Monitoring the Cloud Infrastructure Successfully

In the wake of increased cloud adoption and mounting security threats, how can companies better manage and monitor the cloud infrastructure?

Well, to begin with, organizations must acquire a complete picture of their cyber risk with unified visibility into

assets, vulnerabilities, and exposures, and not siloed visibility caused by using different tools for different assets.

"As the first list of defense against cyber threats, organizations should adopt a risk-based vulnerability management program to continuously monitor their network in real-time while identifying and prioritizing vulnerabilities that could be exploited by bad actors," says Palmer.

He further elaborated that teams can focus on the vulnerabilities and assets that matter most by taking a risk-based approach to vulnerability management. It will help them in addressing the business risk of an organization, instead of wasting their valuable time on vulnerabilities that have a low likelihood of being exploited.

As far as Tenable is concerned, the leading cloud computing company is the first in the industry to launch a cloud-based vulnerability management platform to secure the full range of assets in the modern elastic IT environment, including containers and web applications. The company also provides security teams with unified visibility into vulnerabilities and cyber risk across all assets and computing platforms - from IT to cloud to IoT and OT.

According to Mukherjee of Sonicwall, companies often ignore a lot of factors when migrating to the cloud. For most of them, their priority is the flexibility it offers when the entire world is working from home. "Organizations need to be vigilant in terms of protecting sensitive data, making sure that whatever stored on the cloud is compliant and can be protected," he mentioned.

Mukherjee further clarified that knowledge and understanding are crucial aspects. "We assume that employees know what data\information\files is appropriate to store in the cloud, as opposed to an internal server. The insider threat is real, and it is not always a disgruntled employee, as the statistics confirm. People are trying to get their jobs done faster and efficiently. Security isn't their space, and hence they never think about it for 12-16 hours a day. Cybersecurity is our space, where we live 24x7 and ensure that organizations have security controls in place to prevent accidental misuse and data sharing," he reiterated.

Hence, it is important to protect different layers in the cloud, such as Saas that obe can access without a VPN. Furthermore, there are significant problems, with limitless devices, from laptops, iPad's, tablets that open up risks of contamination.

SonicWall, is assisting such businesses transition with ease by providing best-in-class API-based security with low TCO, minimal deployment overhead, and seamless user experience. This enables companies to focus on their business operations while allowing cloud vendors to focus on keeping their functions up and running.

With features such as Visibility, Next-Gen Email Security, Advanced Threat Protection, Data Security, and Compliance, SonicWall Cloud App Security solution delivers out-of-band scanning of traffic to sanctioned as well as unsanctioned SaaS applications. It further does this with the help of APIs and traffic log analysis. The solution seamlessly integrates with the SaaS applications that have been sanctioned using native APIs, providing CASB functionalities such as visibility, advanced threat protection, data loss prevention, and compliance.

To Sum Up

With more and more people working from home during the pandemic, the abrupt shift to remote working has sparked an unprecedented increase in cyber threats as opportunistic hackers take advantage of the boundary-less ecosystem. Given the present situation, enterprises and cloud administrators need to develop an in-depth understanding of how their organizations use the cloud, as that will further help them to implement appropriate security solutions, policies as well as standards, alongside enforceable roles as well as accountabilities.

When done right, it will help them to prevent data breaches, unauthorized network access, spot threats, and vulnerabilities, encrypt communications, and more importantly ensure uptime for their organizations.

UAE GEARING UP TO THE NEED TO SECURE THE CLOUD

Cloud security is a suite solutions or products that offer security to cloud computing architectures and Cloud based Services. It offers vulnerability scanning, intrusion detection, Data leak prevention, encryption, Identity Governance, identity Access Management, DMARC, endpoint monitoring, and application and messaging security.

"The more data you put on the cloud, there is an imminent requirement of having a cloud security solution which is what we are seeing as a trend and an increase of adoption CASB (Cloud Access Security Broker) solutions," opines K. S. Parag - Managing Director, FVC.

According to the State of Cloud Security 2020 survey done by Sophos, almost 75% of UAE organizations experienced a public cloud security incident in 2019. The current level of cloud security is a major concern according to the respondents of the survey.

However it will be prudent to point it out here that the pandemic has accelerated a transformational shift in cybersecurity in UAE. A wave of digital innovation and growth in usage of cloud-based resources was starting to sweep across UAE when it was suddenly hit by COVID-19 and the latter brought about significant trends such as adoption of cloud delivered security, reviewing remote access policies and tools, migration to cloud data centers and SaaS applications, and

digitization efforts in general.

"There is a constant and deep structural change as customers pivot away from archaic architectures that were designed with what have now become outdated principles in terms of user access, data storage and working environments," explains Mohamed Abdallah, Regional Director - Middle East, Turkey & Africa, SonicWall. "At SonicWall, we work with a vast range of organizations, including government, healthcare, retail and universities. We haven't seen a single organization that hasn't re-engineered their business models and networks to adapt to the 'new normal'."

Cloud adoption in UAE

Cloud services are on the rise across the GCC as the pandemic has forced organizations to make radical decisions about business transformation, cost and risk. There have been a lot of employees working from home, often for the first time, and cloud tools are coming handy for staff productivity and to serve customers.

"There is an increasing reliance on virtual/cloud-based technologies to help businesses scale and reduce their capital expenditure on IT infrastructure.Cloud-delivered security services are on the rise too with the growing usage of remote office technology. Technologies like Secure Access Service Edge (SASE) allows organizations better protect mobile workers and cloud applications," observes Abdallah.

"UAE companies have initiatives underway to move applications out of the public cloud and on to premises' infrastructure," cites Parag.

He however points out that UAE has one of the lowest percentages of hybrid cloud usage today and its projections of hybrid cloud growth 24 months out lag EMEA and global expectations. "The country plans to catch up with the rest of the world within four to six years, when they project hybrid cloud penetration. Perhaps as an interim step to hybrid cloud, UAE companies currently deploy far more workloads and applications on private cloud than any other platform and do so more than most other countries," believes Parag.

As mentioned, the COVID-19 crisis has

K. S. PARAG, Managing Director, FVC

MOHAMED ABDALLAH,
Regional Director - Middle East, Turkey & Africa, SonicWall

triggered an increase in demand for Digital Transformation across different sectors in UAE. "Good news is we are seeing organisations re-assessing their cloud adoption strategies and cloud readiness, pivoting quickly to digital solutions and tools to ensure Business Continuity, be it distance learning or working remotely using teleconferencing," says Parag.

Present state of Cloud security

The COVID-19 pandemic while has been a challenging time for businesses because of the historic disruption that has accompanied; it's been a boon for cybercriminals. The risk surface got hugely extended, and the need of the hour for organizations is to look at prioritizing cyber security technologies and adapting to a hybrid cloud-ready cyber resilience strategy. This is true not only in the UAE market but also globally.

According to a recent update, the UAE's Telecommunications Regulatory Authority (TRA) is working on cybersecurity policy for a cloud-based future, according to Eng Abdulrahman Almarzouqi, Director of Cybersecurity, TRA. The TRA meanwhile is actively working with other organisations including international bodies such as the International Telecommunications Union to ensure that its policies are in line with international standards and practices.

"Layering cloud defenses while building a continuity and backup plan can help organizations quickly return to standard operations without losing critical data or productivity," cautions Abdallah. "In fact, SonicWall's recently launched Mid-Year Threat Report showed a dramatic increase in phishing and ransomware over the last few months, with financial gain emerging as an increasingly important motivation as the economic damage of COVID-19 becomes apparent. Organizations should therefore be on the lookout for next-gen security solutions that can seamlessly integrate with SaaS applications and offer shadow IT visibility and control for cloud usage on the network."

"As much as cloud computing has helped with the storage of data, it has created the need for increased security. Without testing, backups and proper access permissions, data can be easily hacked or stolen, which is leading to an increased awareness amongst customers and they need to get equipped with these capabilities," says Parag.

And so…

Now that everything is moving to the cloud, as is evident during the pandemic, it is never too late to drive a cloud-driven future. Security of the cloud therefore should be the topmost priority of every organization dealing with data on the cloud.

However concerns revolving around lack of internal IT skills and retaining qualified IT staff continue to loom large for UAE companies. In fact UAE respondents have agreed that they lack the internal IT skills required to meet business demands and the inability to retain IT talent were higher than the global averages. This in turn might slow the progress in adoption of the cloud in the UAE.

But on the brighter side of things, the shortage of skilled security practitioners has driven the use of more security process automation. Approaches include more automation of security tasks and support through managed service to ensure that no critical security controls are dropped.

A recent forecast by Gartner reveals that Middle East and North Africa (MENA) enterprise information security and risk management spending will total US$1.7 billion in 2020, an increase of 10.7 percent from 2019. This increase in spending is an evidence of how companies are slowly gearing up to the importance of securing not only their networks and endpoint devices but will also look to secure the cloud in future.

Digitaltech Media

Inform, Inspire, Innovate!

WHAT DO WE OFFER?

Digital Marketing

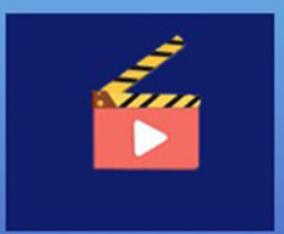
Content Writing

Marketing Collateral

Consulting

Events & Audience Acquisition

Branding



Video & Animation

Designing

Lead Generation

EDM / Banner Design

Visit us - www.digitaltechmedia.in

Contact us for advertisement, video & our services - info@digitaltechmedia.in