Digitaltech Media
Inform, Inspire, Innovate!

• Vol 1 • Issue 11 • May 2021

Bobby Gupta - A Visionary Leader in the Making

TRENDING STORY
Where Does India Stand in the AI Race?

UAE MARKETSCAPE
DDoS Attacks in UAE See a Spurt in the Wake of the Pandemic

PRODUCT REVIEW
Virsec Protects The All Runtime Elements Of Host Workloads Running In Vms Or Containers

WE ARE TURNING ONE!

Coming soon

Digitaltech Media

Inform, Inspire, Innovate!

Anniversary Special Edition!

Watch this space for more...

SERVER SECURITY

VIRSEC

Protecting Application Workloads from the Inside.

Our unique technology stops the widest range of cyberattacks during runtime without signatures, delivering unprecedented accuracy and lowering operational costs.

NO Dwell-Time

NO False Alerts

NO Learning, Tuning or Noise

Stop Fileless Memory Attacks | Protect Legacy Applications | Reduce Patching Urgency | Engineered for Servers—Not Endpoints

"We are at the inflection point for the next paradigm shift in cybersecurity and Virsec does what is needed: protect application workloads at runtime. This is the new battleground."
– **John Chambers,** Virsec Investor and Strategic Advisor and Former Cisco CEO

We invite you to learn more: **virsec.com** | **info@virsec.com**

Bobby Gupta – Carving his Niche as a Trendsetter in the Technology space

Bobby Gupta, who is the SVP & MD – International Sales & Corporate Development at Virsec is a firm believer of one thing – that if you want people to take notice of you then you should have the dare to dream big. Because as someone rightly said - "If people aren't laughing at your dreams, your dreams aren't big enough."

For someone like him who understands the value of setting up the BHAG (Big Hairy Audacious Goal), Bobby has always learnt to be an innovator when it comes to sales and GTM strategies. "I simply follow Ray Dalio's formula - have a clear goal, identify problems, diagnose problems, design a plan and then push through to completion," says Bobby.

After earning his Engineering degree from India, Bobby Gupta did his MBA from Australia. Luckily for him, Bobby got his big break during the early stages of his career with IBM in Australia.

"During my ten years at IBM, I worked in various capacities starting from individual sales to the sales manager role in the Software Group, IBM Global services and IBM Global Tech Services," Bobby recalls. "Thereafter I joined Tech Mahindra as VP Sales for Australia, rising to the position of Sr Vice President Sales for APAC & MEA, before relocating to USA as SVP Sales US West Coast. During my six years with Tech Mahindra, I handled regions from $50m to $500m annual revenue and grew top line every year," he says.

Bobby was also part of the CEO's Global Leadership Management team and was the most successful regional business head before he left Tech Mahindra in 2014 to pursue his interest in the startup world.

Current role at Virsec

At Virsec, Bobby runs the entire GTM (Go to market) for international business while being responsible for sales, pre sales, marketing, alliances, channel partners and strategic partnerships. He is also a part of the Virsec corporate development team, driving key corporate initiatives along with the CEO, Dave Furneaux.

VIRSEC

Bobby Gupta
SVP & MD –
International Sales
& Corporate Development,
Virsec

"I joined Virsec even before the product was built and in a matter of just 3 years we have seen its fast adoption with our Government, Banking, Telco and large infrastructure clients. We now have physical presence in 6 countries, and our product is deployed in around 16 countries. We have plans to expand to 25 countries by end of 2021," asserts Bobby.

Virsec as a cyber security company is uniquely positioned to disrupt the application aware workload protection industry. The company has recently been awarded the Hot Company in the application aware workload protection category, Most Innovative in cloud workload protection, Hot Company in container security and Best Product in runtime memory protection.

A startup Mentor –
another feather in his cap

Besides working for Virsec, Bobby wears another hat as an advisor and consultant to startups. He is engaged as a mentor and as a board advisor to several startups in the field of cybersecurity, AI, Big Data, analytics in the San Francisco Bay Area.

"So I am also an angel and seed investor," Bobby says with a twinkle in his eyes.

So where did this inspiration come from?

"Putting up in Silicon Valley has really inspired me of what I do. This is the only place in the whole world that has given rise to key innovators and industry shapers, the likes of Steve Jobs (Apple), Elon Musk (Tesla, Space X, Solar City), Redd Hastings (Netflix) and companies like Facebook, Google, Salesforce, HP, Oracle etc have come up that later went on to change the lifestyle of everyone.

There is so much concentration of talent here that ideas keep coming and you can find abundance of people to back you up with seed money."

Bobby explains that every startup, once the product is built needs help with early POCs and global expansion.With his 25 years of experience of running sales globally, it comes handy for him in helping early stage companies for their global expansion. With the Cybersecurity industry booming very fast, Bobby plans to keep helping the clients globally with right protection against cyberattacks by bringing the latest technologies in cyber defence.

"I also see a big uptake in AI/ ML in healthcare and fintech and so a lot of exciting work is happening in the startup world," Bobby predicts.

A TiE charter member and a frequent speaker at various conferences/events around the globe, Bobby however does not deny of having seen challenges during his entire career.

"Challenges are always there in the corporate world whether you are working for a large global conglomerate or a startup," he says. "But if you have a clear thought process, it really helps to come out of a difficult situation faster. I strongly believe in remaining focused, believing in oneself and having clear goals," Bobby sums up.

VIDEO

Where Does India Stand in the AI Race?

Artificial Intelligence (AI) can dramatically transform the way we function, lead our life and conduct ourselves in private and public. AI can boost success and productivity for organizations and individuals. A report from NASSCOM suggests that Data and Artificial Intelligence (AI) can add $450-500 billion to India's GDP by 2025 while driving economic growth.

This clearly indicates that India is one of the prominent drivers of the AI revolution. Many Indian companies and also start-ups have started creating AI solutions to cater to different segments including, IT/ITes, Telecom, manufacturing, healthcare, BFSI, hospitality, and education among others.

But where does India stand in the AI Race? Also, how has the pandemic accelerated the need for Artificial Intelligence and AI-based applications and automation solutions currently being offered by Indian companies and start-ups?

These are some of the key questions that need addressing.
Read on to find out more.

AI and How the Pandemic is Accelerating the Adoption of the Technology?

VISWANATH RAMASWAMY
Vice President, Technology,
IBM Technology Sales,
India/South Asia

In essence, AI looks to imitate the way the human mind and intelligence functions. AI applications use powerful algorithms while digesting humungous amounts of data for pattern identification. These provide users with several crucial insights, much-needed for the growth and success of their business or operation.

According to Viswanath Ramaswamy, Vice President, Technology, IBM Technology Sales, India/South Asia, "Companies are embracing digital technologies as a means for driving meaningful and substantive change within their business. They are looking at speed, efficiency, and innovation to stay ahead of the competition.

Trusted AI, the rise of virtual agents using NLP, automation, and anywhere Hybrid are the top areas that have emerged as key business enablers in the last year owing to the acceleration of technology adoption."

Apart from this, the pandemic has also forced Indian businesses to embrace innovation and move towards emerging technologies like AI to reimagine their functioning, making them more agile and flexible. While the country continues to battle Covid-19, firms continue to focus on AI to prepare for the new normal.

GLOBAL AI ADOPTION INDEX 2021

INDIA REPORT

IBM.

78%

think it is very important to their company that they can **build and run their AI projects wherever the data resides**

Barriers to AI adoption

52% see limited expertise or knowledge as a key barrier

50% see increasing data complexity and data silos as a barrier

95%

believe that it is critical to their business that they can trust that their AI's output is **fair, safe and reliable**

53%

report their company has **accelerated rollout of AI due to the COVID-19 pandemic**

62%

are most likely to say **driving great efficiencies in processes and tasks** as the key reason that their company is using / considering using automation software or tools

43%

say that the COVID-19 pandemic has increased their focus on **security and threats**

54%

need a **better way to interact with customers** which influenced their decision to use automation software or tools as a result of the COVID-19

MATTHEW OOSTVEEN
VP and CTO,
Asia Pacific & Japan,
Pure Storage

Echoing similar sentiments, Matthew Oostveen, VP and CTO, Asia Pacific & Japan, Pure Storage, explains that the pandemic has only accelerated the adoption of AI as organizations realize the importance of calibrating business plans with AI strategies.

"The array of industry-specific tech solutions backed by emerging technologies like the Internet of Things, Robotics, Blockchain, and more are being powered by AI algorithms and are also cloud-enabled that helps them reach their maximum potential," Oostveen adds.

AI Adoption Challenges

An Accenture study reveals that AI technology can boost the national growth rate by 1.3% and further add $957 bn by 2035 to the Indian economy.

But, AI adoption challenges are multifaceted and require a holistic approach to solve them. These adoption challenges can be broadly put into 5 different categories, including infrastructure, research, patent, talent, and social concern.

"AI is smart, but when the AI model makes a mistake, you need human intervention. We need human intervention to assess the context in which an algorithm operates and understand the implications of the outcomes," elaborates Oostveen of Pure Storage.

There is substantial demand for professionals who can work on AI algorithms and have relevant skills. But, right now, the demand side surpasses the supply base of skills in this domain.

"In India, some companies believe that the biggest AI adoption challenge is that firms think that AI has no role to play in their corporate culture, while others think it is because there is not enough quality data.

Most of the smaller companies struggle to find good AI talent that can form their in-house AI team," explains Sudhir Goel, Chief Business Officer, Acer India.

SUDHIR GOEL
Chief Business Officer,
Acer India

Key challenges hindering the adoption of AI in India include:

- The quality of available data, as AI systems require good quality data inputs.
- A shortage of talent for roles such as data scientists. India currently has very few researchers in areas such as research production and machine learning.
- Maintaining algorithmic transparency. While Indian organizations may be the custodians of massive amounts of data, unlocking and connecting that information is still a challenge.
- The availability of open-source data is crucial for any country to accelerate AI innovation and adoption. It is crucial to have a cloud computing infrastructure to have seamless availability of data.

"AI solutions build on ML and DL are based on huge volume of confidential data. India is defining its direction with the Personal Data Protection Bill, 2019, and the National Cyber Security Strategy, 2020," shares Naqui Ahmad, Country Manager, NZXT INC., South Asia - APAC.

NAQUI AHMAD
Country Manager,
NZXT INC., South Asia - APAC

Challenges of AI Adoption in India

- India spends only 0.6% of the GDP on R&D. This is a major impediment to the growth of AI in India.
- India also ranked very low in the AI flow index by the Global AI summit 2019.
- The lack of infrastructure for the development of AI in India. Out of the 500 most powerful supercomputers in the world there are only three in India, while the USA and China hold over 100 and 200 respectively. Hence competing with such global powers becomes very challenging.
- India has lacked in the patent department due to the poor definition and enforcement of intellectual property, but that is slowly changing with over 12% of AI IP being patented.
- Other social concerns, such as privacy threats, data security, lack of integrity to be considered.

IBM also believes that while the adoption of AI is poised to grow, some global organizations are still facing several challenges in terms of AI adoption.

An IBM survey further affirms that there are essentially three barriers in the way of AI adoption. These include Limited AI knowledge or expertise (39 percent), increased data silos and data complexity (32 percent), as well as a lack of platforms/tools for creating AI models (28 percent).

"Persistent barriers across markets and industries highlight the need for continued focus on addressing skills and solutions gaps," reiterates Viswanath Ramaswamy of IBM.

But what is even more crucial is that organizations must familiarise themselves with AI and grasp the method to create AI solutions.

Following this, they must build an AI strategy for its implementation into their work culture.

So will 5G speed up the Adoption of AI in India?

AI today has been deployed across business functions like customer service, finance and tax, HR, IT and cybersecurity, manufacturing, and operations, R&D, risk, legal and compliance, sales and marketing, supply chain, and logistics, among others.

The advent of 5G technology will make AI a ubiquitous tool in the world of business. AI, when combined with 5G, will transform the world. 5G is also not only about faster internet and information. It has the potential to change our existing mobile applications and impact all aspects of our life.

VENKAT BOYALLA
CoFounder & Director of Ajna AI

"5G's industry-grade performance makes it easier to connect and utilize cloud and edge computing which will, in turn, give rise to the development of AI. Large data can be stored and processed within the cloud using AI because of the 5G technology," says **Venkat Boyalla, CoFounder & Director of Ajna AI**- a Chennai-based start-up that offers customer behavior analytics platform which helps brick and mortar businesses, including retail, supermarkets, hypermarkets, hotels, hospitality, luxury retail, etc.

Sharing similar thoughts, Sudhir Goel of Acer India clarifies,"The advent of 5G will help India become a global leader in cloud computing and internet-of-things (IoT)."

Vendor Offerings

Given AI's potential and capabilities, vendors are in no mood to lag behind. As a result, IBM is working to accelerate AI adoption by delivering AI solutions designed to match the needs of businesses. The IT giant is also looking to provide organizations, data scientists, and developers the capabilities they require to scale AI.

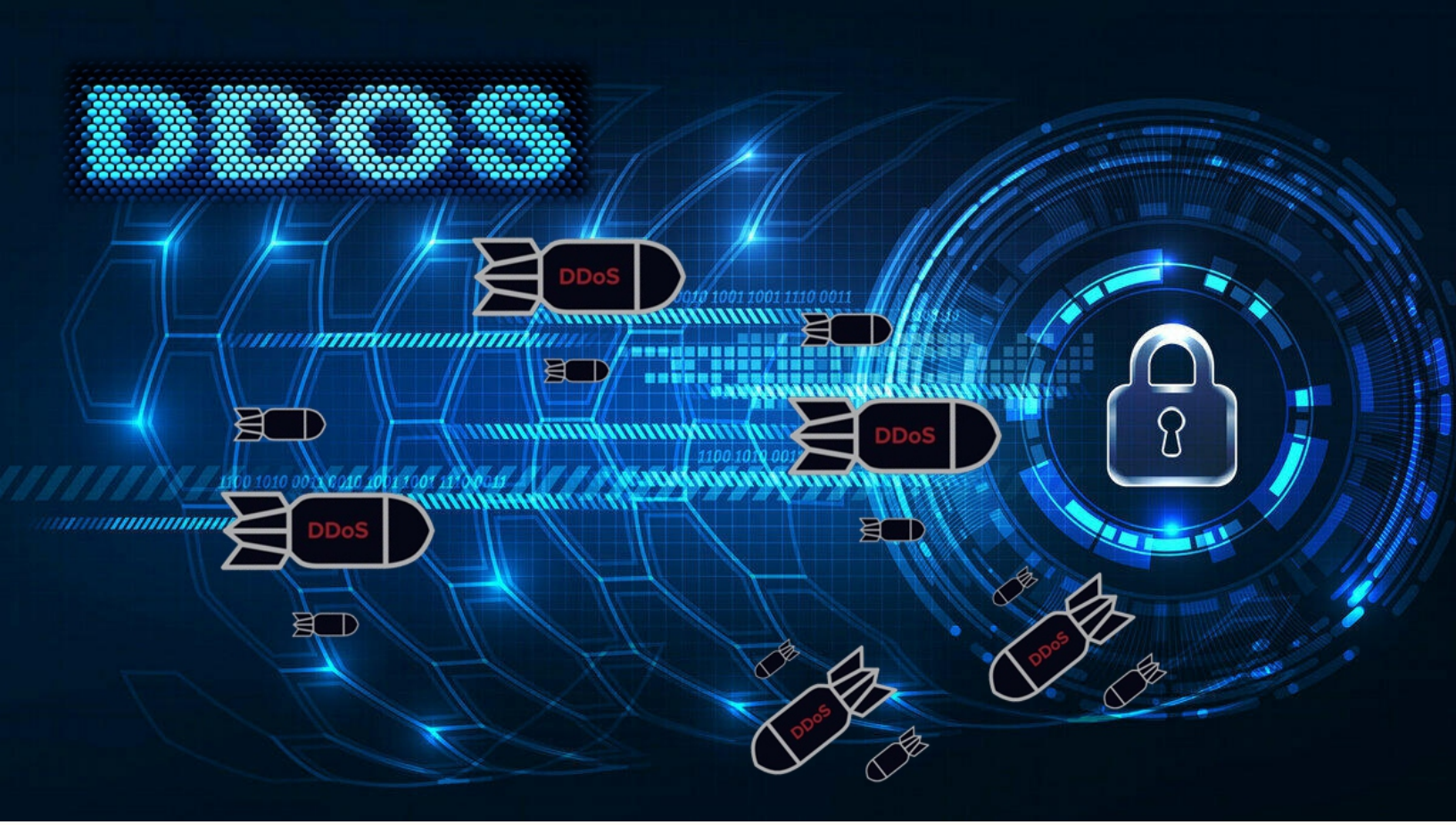
IBM is continually bringing innovations to IBM Watson from IBM Research that help organizations better understand the language of business, automate processes and IT, and drive trust in their AI outcomes. Acer, on the other hand, offers the "aiWorks solution", which is essentially an Artificial Intelligence Computing Platform that offers a streamlined and cost-effective integrated solution for servers, workstations, networks, and storage. The aiWorks solution is designed to offer a robust, resilient, and reliable IT infrastructure making it one of the keystones of a successful business.

Pure Storage is also not far behind. In March 2018, Pure announced AIRI, the industry's first comprehensive AI-Ready infrastructure architected by NVIDIA and Pure Storage. Since the announcement of AIRI, it has been widely deployed in many global industries, including healthcare, financial services, automotive, etc.

Since AIRI paved the way for these organizations to turn data into innovation at an unprecedented pace, it also created the necessity for a highly scalable solution that spans multiple racks of DGX servers and FlashBlades storage.

NZXT, which has over a decade of expertise in developing award-winning, high-quality PC components, focuses on enabling engineers who are experts in their domain but require a flawless PC. The company offers PC components that are reliable and provides a hassle-free user experience.

"Building a PC on NZXT ecosystem lends itself to service life extension by nature of being easily upgraded by the user. You can plot your upgrade pathways in the initial building phases," adds Naqui Ahmad of NZXT.



DDoS Attacks in UAE See a Spurt in the Wake of the Pandemic

DDoS attacks are malicious attempts to break the flow of traffic in the targeted server and overwhelm it. These attacks occur through corrupted links or files, and its goal is to freeze the network and exhaust all resources essentially.

DDoS attacks can result in website and network outages, compromised data, and lost revenue for organizations, both large and small. With the availability of DDoS-as-a-Service tools on the Darknet, the increased vulnerability of IoT devices and the resulting rise of botnets, and financially-motivated hackers launching ransomware campaigns, DDoS assaults have become even more common, powerful and profitable. DDoS protection and DDoS mitigation solutions have therefore become more important.

The State of the Market Report 2021 recently brought out by Help AG, a security organization based in UAE, cited over ten million Distributed Denial of Service (DDoS) attacks globally in 2020. What is even more intriguing is the fact that UAE alone recorded 183% increase in these attacks that targeted mostly government and private enterprises.

Interestingly enough, this has happened for the first time in history of cyberattacks.

Conclusion

India is witnessing unparalleled momentum in the adoption of AI, remote collaboration tools, and digital access to services across industries.

"India ranks third in the world after China and the USA in producing quality AI-based research papers, over 85,000 since 2010. 58% of Indian companies use AI in scale. Every year 6-7 AI-based tech start-ups from India join the unicorn club. But the country still has a long way to go to deploy AI usage on the scale of developed countries," shares Venkat Boyalla, Co-Founder, Director of Ajna AI.

Apart from this, Digital India aims to combine information technology and processes to provide faster services to citizens of the country. Other initiatives such as Aadhar Enabled Payment System and National Mission in Education through ICT are also driving the growth of the AI market in India.

Given the above, it is quite evident that every sector in India is looking to implement AI in their programs, as it has the potential to improve decision-making and solve a plethora of problems.

L ASHOK
Managing Director – Futurenet Technologies

"The changes in the IT landscape in recent years has put a lot of pressure on cyber-security systems in the IT infrastructure," explains L Ashok, Managing Director – Futurenet Technologies. "With the acceleration in cloud adoption across the UAE region, and an increasingly mobile workforce, cyber criminals have found new ways to exploit security weaknesses."

Despite the occurrence of a lot of high profile incidents and increasing awareness around the topic, many companies still consider cyber security very casually. Strangely, even today many companies implement security measures only after getting hit by a cyberattack of any kind.

As a result, this lackadaisical attitude on the part of companies has made these DDoS attacks by far the most prolific form of cyber threats faced by any organization today.

The same report states that these attacks have affected businesses across sectors including government, oil, healthcare and telecom. "Healthcare companies were the prime target for these attacks, preventing people from accessing proper information from health care sites and hospital applications. They found a rapid increase due to the common tactic to disguise DDoS attacks as Covid-19 information links due to the increased traffic to information surrounding the pandemic," observes Ashok.

VIDEO

However, K. S. Parag, Managing Director – FVC is quick to point it out that recently this trend has been changing to now affect small business and Oil & Gas industry and a lot of this has got to do with lack of cyber security awareness and/or weak security systems in place.

K.S. PARAG
Managing Director – FVC

Situation after the pandemic

Help AG's report further points it out that essential sectors such as e-commerce, online learning and healthcare that shifted to digital during the crisis, were particularly targeted by cyber-criminals. The Covid-19 pandemic has forced organizations worldwide to adopt to remote working, due to which mitigating such attacks by the response team is met with slower response which in-turn increases the extent of damage of the attack.

"The biggest challenge that all CISOs in the region have faced during the pandemic has been remote access and to securely provide Work-from-home capability to their business," says Parag. "Additionally with how long this pandemic situation has been enduring, it had to be a sustainable robust system and not a stop-gap arrangement that the off-the-shelf one size fits all hardware technology brings to the fore."

According to him, in today's economically challenging and ever-evolving attack landscape, it becomes even more difficult for the CISO and his team to monitor and thwart any attack on their business processes. "With the advent of cloud adoption now gaining traction in the MEA the challenges are all in the Zero-day category," he adds.

What lies ahead?

While 2020 witnessed a steep rise in the number of cyberattacks and proved to be a busy year for both attackers as well as cybersecurity personnel, 2021 will see such attacks becoming more frequent. These attacks will also be very specific regarding who they target. "International cyber espionage will be one of the main motivators for cyberattacks and we will see security vendors being attacked and compromised at an even greater pace," opines Ashok. "Such attacks will not only create opportunities for newer attacks or variants, but will also drive cybersecurity innovation in 2021.

"There are therefore opportunities galore for the channel community to invest their time in and grow their business during this tough and challenging business climate. Ashok further cites that the partner communities, especially security agencies will grab these opportunities to ensure the security of infrastructure of organizations by adopting to new technologies. These include -

- Establishing a Security Operations Center at the premises
- Providing Security-as-a-Service
- Providing SIEM-as-a-Service for medium and small scale industries which helps them identify such attacks and ensure they are mitigated.
- Adopting to DDoS-as-a-service, where the service provider hosts the websites/applications and also provides DDoS attack prevention, mitigation and response as a whole service.
- Investing in a DDoS Mitigation team, who help organizations as soon as a DDoS attack is identified by the organization as an on-demand basis.

Parag is also of the same view. For him, any business, while rolling out new products and services spreads data across disparate environments. Securing these network environments creates gaps that hackers can exploit easily. A CISO well understands this but a lot of them would need to be convinced before conducting business with a trusted security brand following a breach. And this is where partners can come into the picture. However the good news is that organizations in the UAE are becoming increasingly aware of securing their own data as well as their customers' data after the increase in the number of cyberattacks in the country. They are now seeing the importance of DDoS protection and considering it to be must-have in their first line of defense. There is likely that large investments will be happening in and around securing infrastructure, with surveys reporting the increase in investments to be 10% to 15% in 2021.

How to prevent a DDoS attack?

It is encouraging now to watch that next-gen security companies are moving away from traditional remote access technologies such as VPN etc and providing stand-alone DDoS appliances to the customers' existing Firewalls and other perimeter security solutions. However the following tips will help to avert a devastating DDoS attack -

Keeping ready a DDoS Attack Response Plan:

Have a response plan ready in case of a security breach so your organization can respond as promptly as possible. Additionally, establish an incident response team in case the DDoS is successful and define responsibilities.

Secure your Infrastructure with DDoS Attack Prevention Solutions:

Equip your network, applications, and infrastructure with multi-level protection strategies, combining firewalls, VPN, anti-spam, content filtering and other security layers to monitor activities and identity traffic inconsistencies.

Perform a VAPT (Vulnerability Assessment and Penetration Testing):

A VAPT involves identifying security exposures so you can patch up your infrastructure to be better prepared for a DDoS attack, or for any cybersecurity risks in general.

Identify Warning Signs of a DDoS Attack:

Try to identify the symptoms of a DDoS attack using a log monitoring and alerting tool as early as possible.

VIRSEC

Application-Aware Workload Protection

Runtime protection against advanced cyberattacks

Virsec Protects The All Runtime Elements Of Host Workloads Running In Vms Or Containers

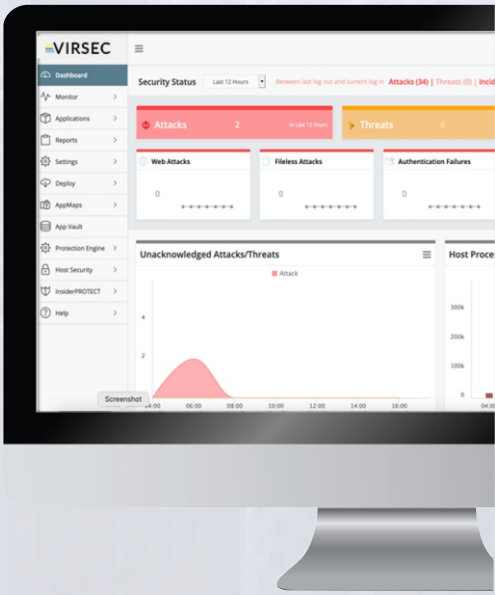
Orgnizations that invested in endpoint protection combined AV and network security contorls to tackle the threats targeting host systems and applications, are now facing critical levels of cyber risk.

A Verizon annual Data Breach Investigation Report concluded that 70% of the attacks are targeted towards server workloads. Moreover, the increased sophistication of ransomware, supply-chain attacks, and dangerous exploits that lead to sabotage, espionage, and business stoppage, has resulted in substantial losses and massive operational costs on a continuum and without the ability to stop events at runtime or prevent them from happening again.

In simple words, with your current approach to protection malicious threat actors accessing your system, can potentially take control of ALL applications, and gain access to confidential, protected, or sensitive data that your business depends on. Can you really turn a blind eye to that?

Now consider a new approach to protecting workloads that is centered on runtime, as offered by Virsec.

Virsec Security Platform (VSP) is designed to stop the most dangerous attacks targeting hosted workloads, systems and applications at runtime with unmatched accuracy and no human effort. VSP is the only single solution that safeguards the entire application surface, focusing visbility and protection across all runtime components throughout Host, Memory, and Web, layers. So, if end-to-end protection of applications is something that you are deeply concerned about, then Virsec Security Platform is the ideal way forward!



VIRSEC

Why Endpoint Technology Fails to safeguard application workloads?

As far as the EDR/EPP tools are concerned, they are designed to address the security needs relative to enterprise app users and endpoint, i.e., smartphones, laptops, PCs, and hand-held tablets, and devices such as modems and routers. But when organizations depend on EDR/EPP solutions for host protection, the result is usually poor. Attack methods that stem from endpoints are much different from the exploit methods applied by residents on the server. Without contextual insight across application packages and an understanding of business logic, you can only use tools like EDR/EPP to analyze events that have transpired, thus investing and hunting behavior deemed suspicious. Cyber attackers are fully aware of the limitations of endpoint security, and thus they tend to attack the server and application workloads with confidence that they have time to achieve a successful outcome.

Below, are five reasons why EDR and EPP technology are not ideal for analyzing application behavior on processes occurring during runtime:

1. Server-based applications and Workloads differ from those that run on endpoint devices.
2. Exploits used to target workloads are not the same attack methods as those aimed at endpoints.
3. EDR/EPP solutions lack strict application controls to keep pace with modern threats and ensure applications only execute as intended.
4. Threat detection approaches focus on identifying suspicious events, using non-deterministic analysis algorithms for detection and supporting reactive security rather than attack protection and threat prevention.
5. Lack of visibility across runtime throughout the application stack, including memory enables attacker to easily bypass endpoint tools.

How Can Virsec Security Platform Solution Help?

Virsec Security Platform (VSP) is designed to block attacks that EDR/EPP tools tend to miss. Virsec stops common and never before seen attacks at the earliest point in the threat cycle no matter how they manifest – preventing exploits from metastasizing and exerting damage downstream.

VIRSEC

NO Dwell-Time

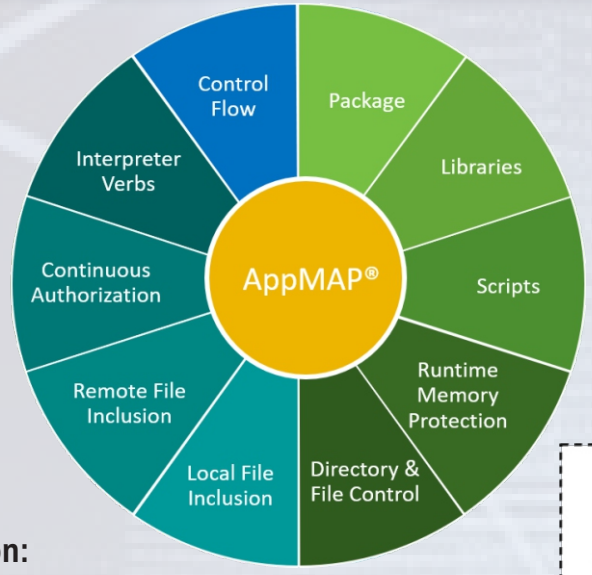
NO False Alerts

NO Learning, Tuning or Noise

Here's how VSP stops advanced attacks:

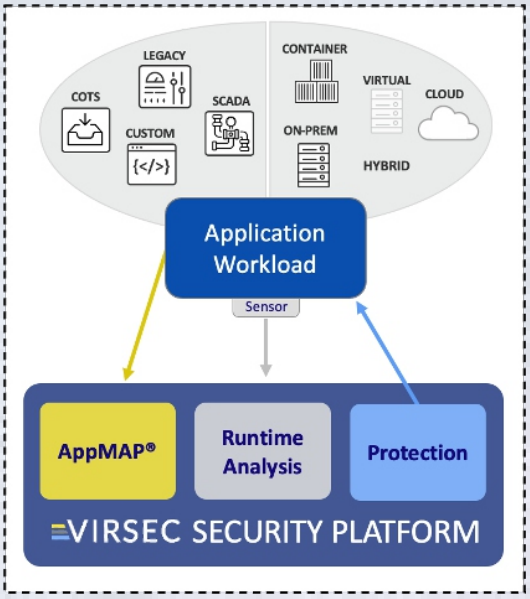
Accurate, Practical, and Effective Approach:

Unlike other solutions that depend on behavioral and heuristics rules for detecting attacks, VSP relies on a code-based, deterministic approach for detecting and protecting against advanced cyberattacks with no tuning, no noise, and no signatures.



Comprehensive Protection

The product is designed to safeguard all the apps, including COTS, customs, legacy, third-party, SCADA, on different platforms such as on-premise, virtual, hybrid, cloud, container.



Advanced Ransomware Protection:

Virsec Security Platform precisely detects complex never before seen ransomware attacks upon the first insurgency within milliseconds and instantly executes protective actions that stop attacks and prevent any disruption or data theft. Because an attacker can infiltrate host environments from various means, VSP protects at any point in the kill-chain, addressing compromised libraries or files, injection attacks, and misuse of memory or commands to facilitate deployment of attacker toolsets and accommodate malicious data encryption.

Comprehensive Supply Chain Protection

With Virsec, you can effectively prevent highly sophisticated supply-chain attacks from exploiting application runtime and memory and ensure malicious code never executes, and without isolating or unplugging the system until the patches are available.

Conclusion

Virsec's app-aware workload protection uniquely enables Zero Trust runtime protection against sophisticated attacks. Organizations worldwide trust Virsec Security Platform to protect mission-critical applications, business services, and infrastructure systems, including healthcare, financial service, defense, government, oil & gas, power, technology, telco, transportation, and more.

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