LAUNCH

YOUR CYBER SECURITY COMPANY

IN INDIA

CODE RED

Security PR Network

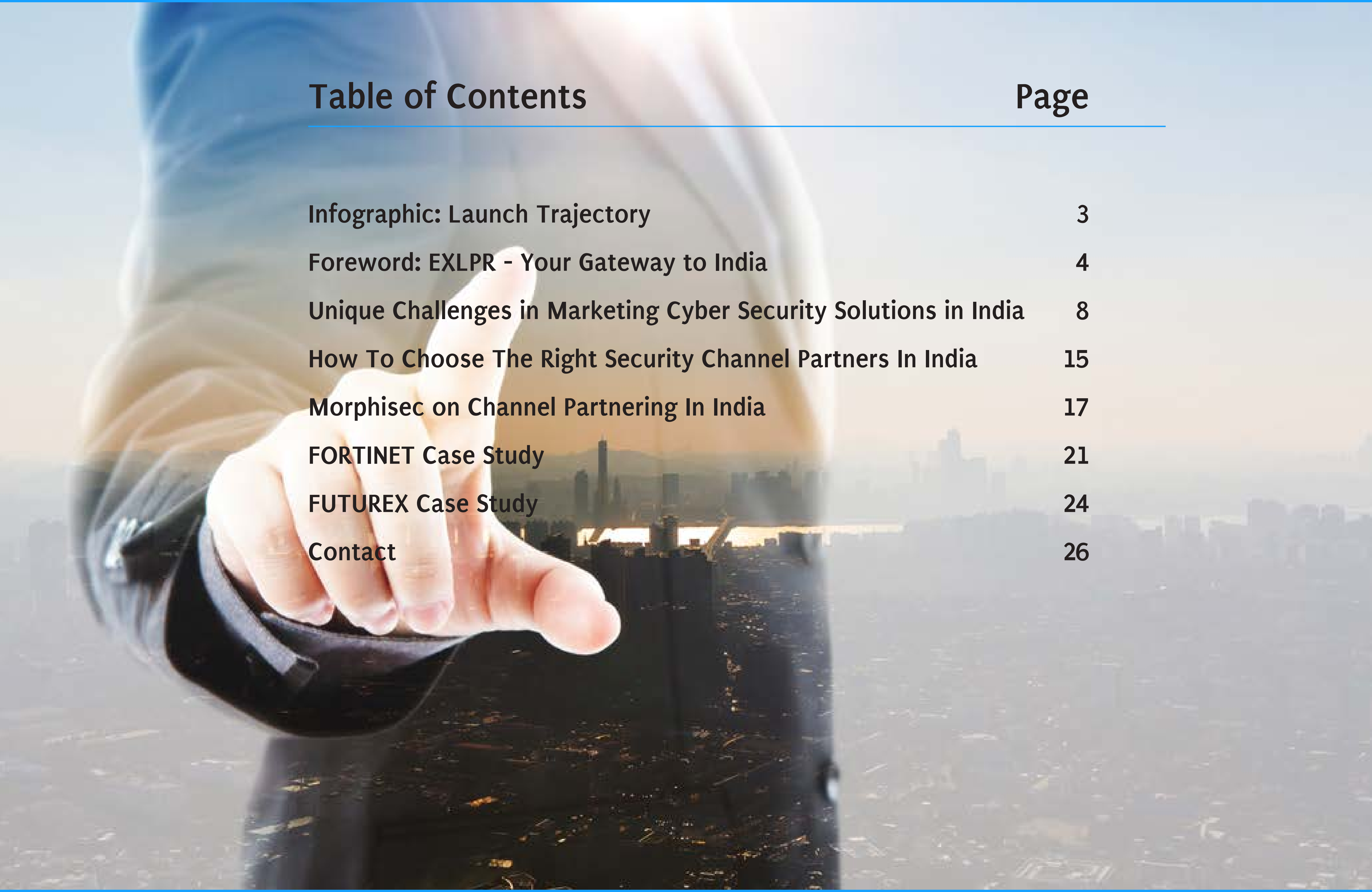
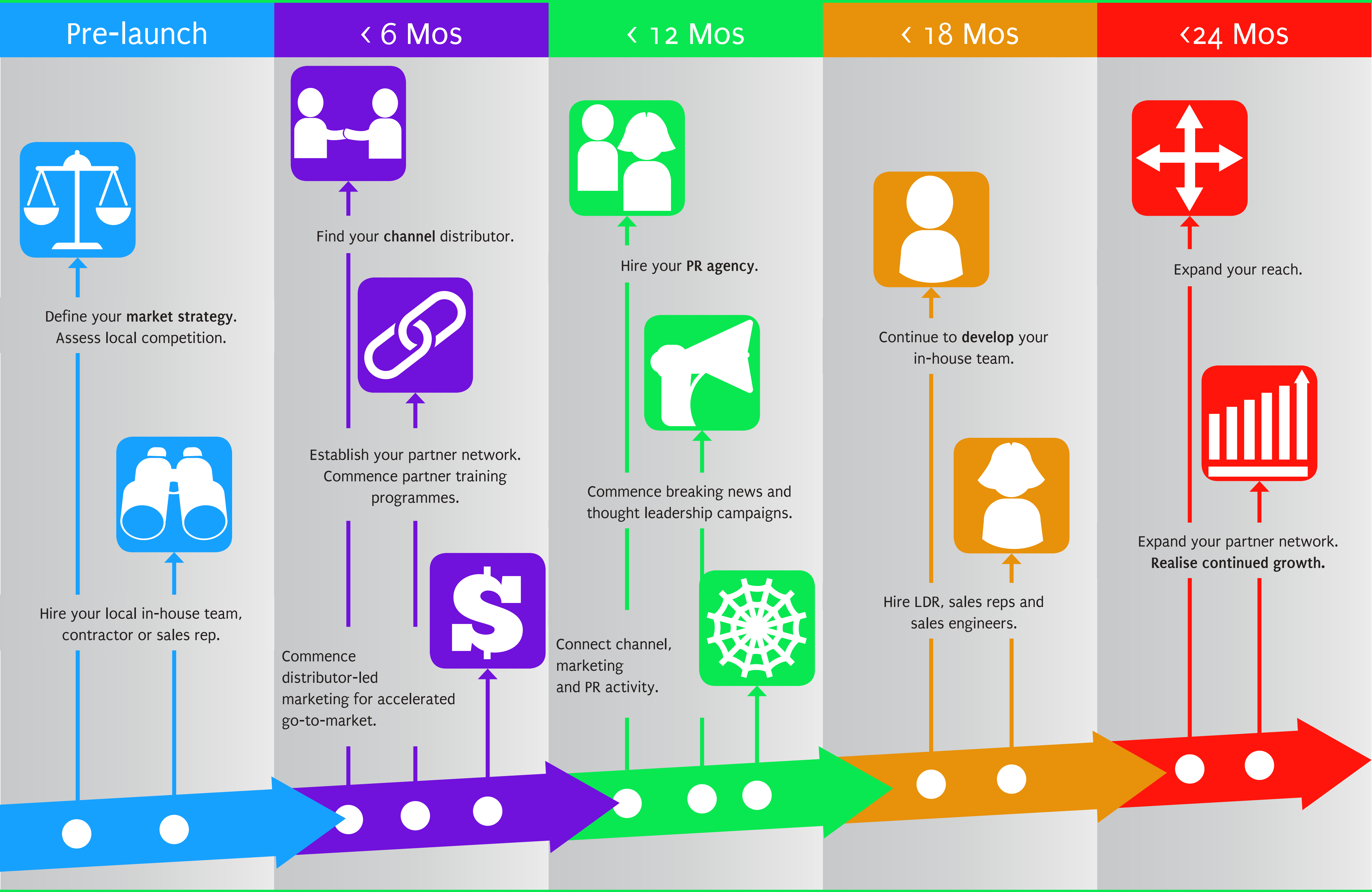


Table of Contents Page

Launch Trajectory



Pre-launch

Define your **market strategy.** Assess local competition.

Hire your local in-house team, contractor or sales rep.

< 6 Mos

Find your **channel** distributor.

Establish your partner network. Commence partner training programmes.

Commence distributor-led marketing for accelerated go-to-market.

< 12 Mos

Hire your **PR agency.**

Commence breaking news and thought leadership campaigns.

Connect channel, marketing and PR activity.

< 18 Mos

Continue to **develop** your in-house team.

Hire LDR, sales reps and sales engineers.

<24 Mos

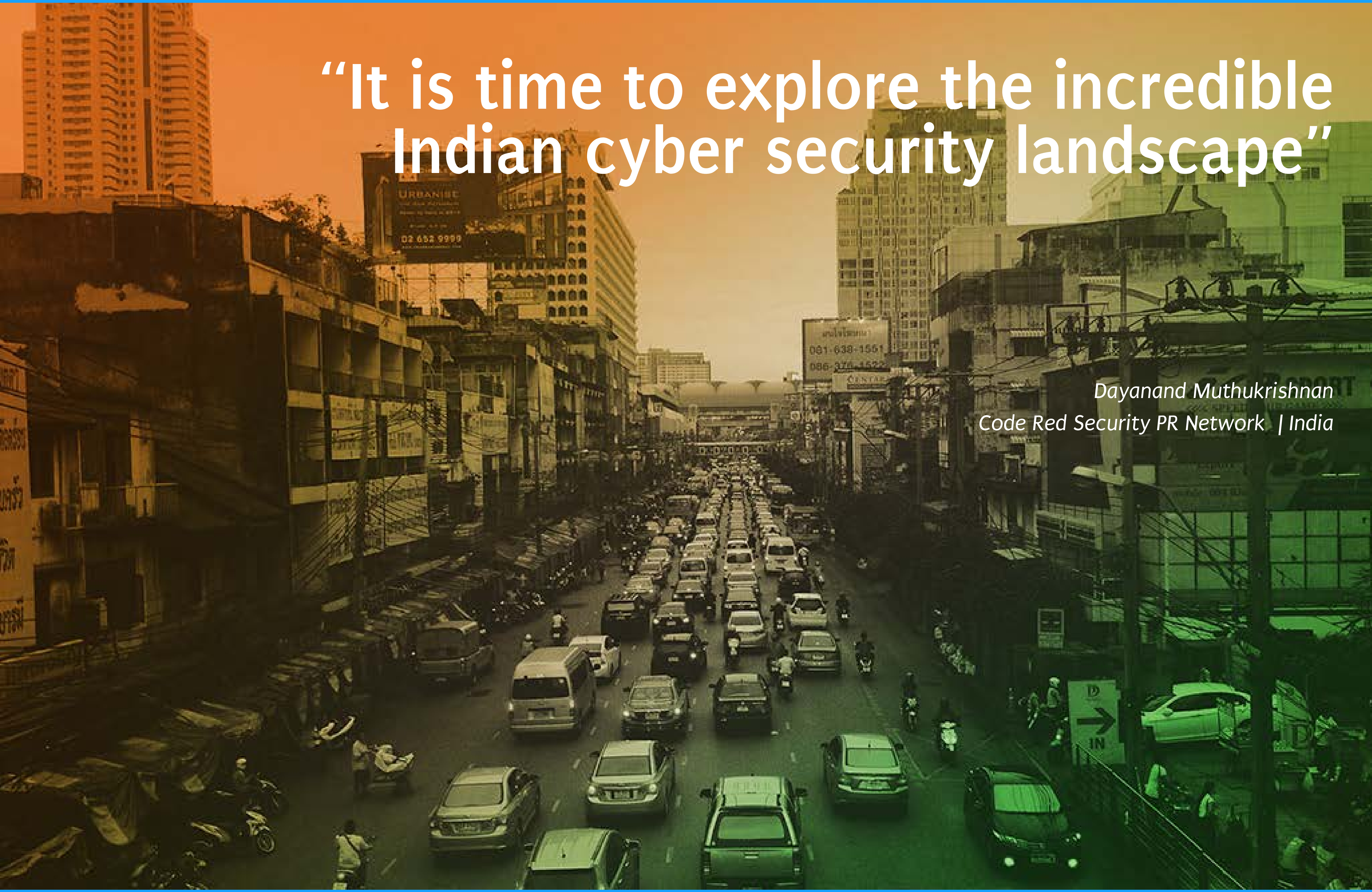
Expand your reach.

Expand your partner network. **Realise continued growth.**

CODE RED

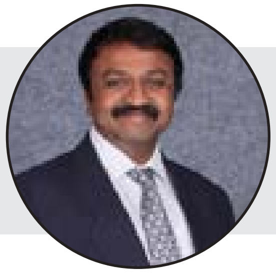
We are ready to help you!

Contact Code Red India today



“It is time to explore the incredible Indian cyber security landscape”

Dayanand Muthukrishnan
Code Red Security PR Network | India



Dayanand Muthukrishnan

Code Red Security PR Network

A cookie-cutter approach to marketing cyber security solutions rarely works, more so in India than anywhere else. A common misconception is the idea of making an "India Strategy" which mistakenly shapes the landscape into one homogenous market.

"The landscape in India for cyber security products, solutions and services is unique. The biggest challenge lies in solving a particular customer pain point. A customer will only adopt a service or solution if they can see the value. And it is tough convincing a client. It's like asking them take a pill today so tomorrow they don't have a problem," says Ajit Pillai, Country Manager, Morphisec India.

But thanks to continuous education by vendors and the market realities they operate in, customers have slowly begun to understand the evolving threat landscape. Having experienced numerous pain points, customers who earlier could not even say that they had been attacked or compromised, today actually share whatever has been compromised with their peers and discuss the ideal form of protection strategy with them.

> **This is a market that rewards long term relationships, built on positive experiences and deliverables.**

Strategic planning, due diligence, consistent follow-ups, and, perhaps most importantly, patience and commitment are pre-requisites for successfully marketing cyber security solutions in India. This is a market that rewards long term relationships, built on positive experiences and deliverables.

Technology wise, India's cyber security needs are not very different from that of the rest of the world. To be successful, requires careful analysis of customer preferences, available budgets, preferred channels, and changes in distribution and marketing practices, all of which are continually evolving.

Dayanand Muthukrishnan

Code Red Security PR Network

After a careful analysis, we propose a few best practices to enter and successfully compete in the rapidly growing India cyber security market:

A Customer First Approach

Instead of focusing on how you fare against competition, present the value you offer to your customers and resellers. By thinking "customer backwards", you better empathize with customer pain points and offer the correct solution for both the near and the longer term, something that Indian customers value big time.

Localize Your Global Strategies

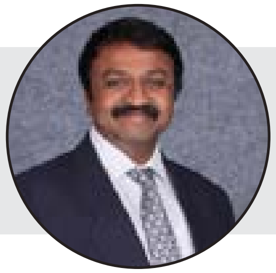
By creating customized local offerings developed from the ground up for the Indian market, you set yourself up for the long haul the right way. In case you can't, the next best thing is to try to adapt your global strategies to local sensitivities in part to ward off stiff competition from homegrown local brands and startups.

Drive Brand Awareness Activities

Often I have heard businesses say, especially consumer security software brands, that they won't be focusing on building a strong brand profile and connect in India as they have licensed their products very "attractively" to a local distributor. The expectation at the brand side is that the local distributor will invest its hard earned margin in building a brand that it has no control over. This approach harms the brand in the long run. Distributors are not able to do brand messaging as trained, specialized brand representatives are. Also, if the brand were to add another distributor or remove the existing one, it runs the risk of a backlash and damage to its reputation in the marketplace.

Make It Easier To Connect With You

Brand reputation always precedes local presence. Word of mouth publicity, social media and Internet ensure that.



Dayanand Muthukrishnan

Code Red Security PR Network

Ensuring that customers and partners know how to get in touch with you is just the most basic first step. You must, additionally, ensure that a trained and well tested response mechanism is ready and at hand to respond. Simple things like a IP based toll free number, email ID that works, go a long way in building a strong brand connection.

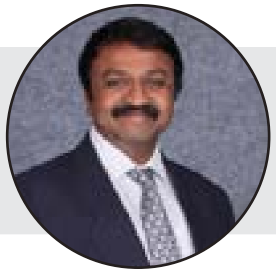
Stay Invested For The Longer Term

Study the market carefully. If necessary engage a Go-To-Market expert to present market opportunities and challenges in greater detail before making a decision to enter the rewarding but challenging Indian market. Once in, have a clear three to four year roadmap for rollout and stay with it. Anything less will mean you will create an impression that could hurt your brand reputation.

Choose The Right Talent And Partners

To succeed you need strong brand champions, both within and outside. Low hanging fruits are not always enjoyable. Choose the right leader and carefully study thier ability to drive brand opportunity, sales and marketing before asking them to drive your brand's fortunes in the Indian market. And offer them PR training at least once a year. The same is true for distributors, SIs and VARs. Strong partners will work hard to open doors for you because of the value your products/solutions deliver to their customer base, both existing and prospective. If necessary engage a Go-To-Market expert to present suitable partners for you to review and engage.

Unique Challenges in Marketing Cyber Security Solutions in India



Dayanand Muthukrishnan

Code Red Security PR Network

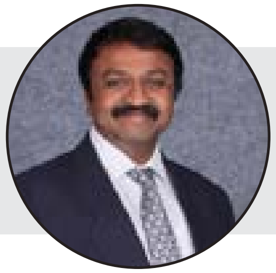
Technology rules every aspect of our lives today, blurring lines between traditional and the modern, connecting people seamlessly, transforming the way we work, bank, communicate, commute, educate, entertain and even how we interact with the government and its various institutions, on a day-to-day basis.

To leapfrog a predominantly agrarian economy into a multi-faceted, technology enabled $ 5Trillion economy by 2025, the Indian government is leaving no stone unturned in its efforts to embed technology into every aspect of its citizen-facing services, particularly in areas such as digital payments, Internet banking, e-governance, personal and business tax simplification & compliance, digital literacy, direct-to-citizen delivery of subsidies, digitization of land records, telemedicine and much more, in an effort to rapidly bridge the digital divide and bring much needed economic benefits especially to those in remote and rural areas of India.

India has the 2nd largest smartphone user base, more than 400 million users, and Internet user base in the world, more than 12% of the world's 3.2Billion users. Driven in part by constantly reducing rates per MB for 4G Internet services and easy availability of affordable smartphones, more than 90% access the Internet, to work, shop, commute, communicate, play and entertain, through their smartphones. And this is driving digital transformation like never before. The following facts illustrate this clearly:

- Mobile banking transactions have grown multifold removing hurdles to physical banking especially in rural areas, lowering cost per banking transaction to a under one rupee, improving bank profitability and as such the banking sector's ability to extend credit overall.

> **India has the 2nd largest smartphone user base, more than 400 million users, and Internet user base in the world,...**



Dayanand Muthukrishnan

Code Red Security PR Network

- India is expected to clock the fastest growth in digital payments transaction value between 2019 and 2023 with a compounded annual growth of 20.2%. The rise of digital commerce, innovation in payments technologies using AI, blockchain, the Internet of Things (IoT) and real-time payments and the introduction of mobile point of sale (POS) devices have also contributed to growth. Digital wallets are not just enabling easy payments for services but promote easy peer-to-peer lending. The government's wish to becoming a true cashless economy in the next few years, is becoming a reality.

However, There is No Light Without Shadow

Rapid digitalization and growing use of everything digital has given rise to a sprawling cyber crime market in India. India presently ranks 5th in the world in terms for DNS hijack and experienced a 457% rise in reported cyber crimes over the last six years including crimes such as cyber extortion, credit card frauds, DDOS, botnets, identity theft, phishing attacks, cyber stalking, and social engineering, from both state and non-state actors and from within and outside the enterprise. Attacks are increasingly sophisticated and a reported 76% of victims are business enterprises. Look at these cases:

- A terminal at Jawaharlal Nehru Port Trust, India's largest container port, suffered a massive attack initiated through a malware called Petya.
- An oil and gas company suffered a phishing attack when email credentials of its senior officials were duplicated to deceive a major client to transfer huge amounts to the hacker's account.

Companies, especially those who hold vast quantities of data either on premise or off site including in the cloud are particularly vulnerable. A recent report revealed that 69% of Indian companies are at risk of a cyber attack. Cyber crime does not spare individuals either. Analysts believe as many as 76% of Indians have been victims of cyber crime and over 60% victimized by computer viruses and malware. But many never report the crime to avoid social stigma and loss of face.

Fighting Cyber Crime in India

To protect the nation against cyber warfare and threats from state actors operating far beyond the country's borders, the Government of India is creating a new tri-service defense agency that will work in coordination with the National Cyber Security Advisor and have more than 1,000 experts distributed into a number of formations of the Army, Navy and Indian Air force.

To tackle domestic threats a specialized unit called the Indian Computer Emergency Response Team (CERT-In) has been operational, since 2004, as a national agency for cyber security incident response and is actively involved with mitigating cyber crimes in India. To give sharper teeth to cybercrime laws, the Information Technology Act of 2008 was amended to cover broader security related issues. The government also plans to table the Personal Data Protection Bill 2018, inspired by the GDPR of the European Union, in the parliament soon.

The National Cyber Security Policy, announced in 2013, integrates all government initiatives to tackle cybercrimes and initiatives such National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC), and sector specific Computer Emergency Response Teams under CERT-In were implemented under the above policy. The Government has also gone ahead and empanelled security auditors for conducting security audits by both government and private companies.

On the business front, cyber security investments are growing. The Aricent-ASSOCHAM-NEC joint study estimated the cyber security market in India to grow at a compounded annual growth rate of 36.2 per cent between 2017 and 2021.

The key to preparedness, industry experts agree, lies in adopting next-gen solutions in the near term to protect the enterprise in the longer term.

> **To give sharper teeth to cyber crime laws, the Information Technology Act of 2008 was amended to cover broader security related issues.**

Evolving Threat Landscape

"Threats today are polymorphic – they do not have one, but many close up," says Ajit Pillai, Country Manager, Morphisec India. In this dynamic scenario, often it is quite possible that enterprises do not know if they have been breached or, worse, how to react once they are attacked.

Lack of Awareness

"There is a worrying lack of awareness about cyber laws and regulations at both corporate levels as well as individual levels. Product features and technical understanding of basic cyber security constructs especially are superficial amongst SMB and individual consumers leading to them making purchase decisions based on peer references or low price points," says Adam Carson, Director of Product Marketing, Futurex.

Adhocism

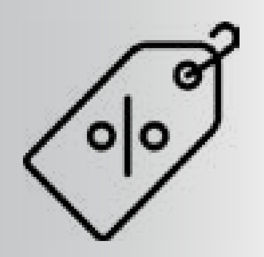
"The cyber threat landscape is multi-layered and highly sophisticated and requires long term strategies. Due to misconceptions and lack of awareness on how solutions are deployed, both enterprise-level and individual level consumers tend to make piecemeal purchasing decisions," says Jayont Sharma, Sanzar Group, Distributor of Avast in India.

Limited Budgets

"Budget constraints are one of the most common reasons quoted by enterprise-level purchase decision -makers when it comes to buying cyber security solutions. Insufficient and inflexible budget allocations mean solutions/products are purchased in bulk at the beginning of a quarter and in the case of an attack mid-year, have insufficient monetary resources to seek out more effective solutions," says Ajit Pillai, Country Manager, Morphisec India.

"It is difficult for IT managers or business owners to keep budgeting for ever growing technology. It is a big challenge, but at the same time they also tend to prioritize based on the threat landscaping, and that's when we see a lot of convincing targeted at the board members and the Chief Revenue Officers in order to get them to allocate additional budgets. The CFOs also seem to get involved in certain business critical protection areas. So we see that there has been a lot of change and it is a challenge for businesses because they have already budgeted for the year and something comes up, they find it very difficult to reallocate budgets" says Ajit Pillai, Country Manager, Morphisec India.

Price Sensitivity



"As observed with the smartphone industry, the Indian audience is extremely price-sensitive. Cyber Security as an environment consists of technology and implementation by the people and the procedures that need to be followed. There is a cost associated with all the three areas and budget constraints negatively impact the adoption of cyber security systems. In such a situation, organizations prefer to procure older technologies or deploy off-the-shelf products that are more economical "than splurge on tailored solutions," says Jayont Sharma, Sanzar Group, Distributor of Avast in India.

Compliance First, Security Next

“What we see is that customers are not very proactive. Except in some of the new-gen business models, they will not change from their usual way of buying. For example for cyber security solutions there are three or four technologies they usually budget for at the beginning of the year. They have some 20 or 30 odd components which they actually position at Phase 1 and when they go for IRT services they might add additional four or five solutions for Phase 2. All this is driven by compliance so that is really the first priority – it could be compliance driven by RBI in the banking sector’s case, or in the insurance sector’s case it could be the IRDAI, if its Telecoms it might be TRAI, and in the case of government it could be govt cyber security policy. It is still a highly compliance-driven process and that is the reason why the buying patterns are aligned with the sector-specific guidelines. Customers go for technologies to comply with the guidelines first, followed by defense. This has always been a challenge for the cyber security industry,” says Ajit Pillai, Country Manager, Morphisec India.

“At the enterprise level, decision-makers like to follow set purchasing patterns and policies that fulfill compliance demands as opposed to proactively seeking solutions that will protect valuable assets against threats, technologies that help protect assets as per the laid-down guidelines come first, defense next”says Adam Cason, Director of Product Marketing, Futurex.

Shortage of Security Professionals

“Although India is rife with a young workforce with considerable IT prowess; there is a dearth of talent when it comes to specific niches, such as Cyber Security. The demand for talented and skilled labor in India far outstrips supply, and with the market poised to grow further substantially, this gap is likely to widen further,”says Ajit Pillai, Country Manager, Morphisec India.

How to Choose the Right Security Channel Partners in India

Dayanand Muthukrishnan

Code Red Security PR Network

Channel partnering is vital to conducting a successful cyber security business in India. The channel partner ecosystem extends reach for vendors while enabling them to package and deliver differentiated solutions needed by various customer segments. Channel partners also provide deep insights about the local market and demand forecasts of customer audiences.

The right security channel partner becomes the face of the vendor company and is able to influence potential customers into permanent ones.

So, what should cyber security companies keep in mind before choosing the right channel partner in India?

Identifying the Ideal Partner Type

It's important to identify the ideal partner type for the needs and the relevant opportunity associated for increased scale, sales and service coverage. The ideal partner is one whose system matches the vendor company's end goal whether its sales reach, product/service delivery and implementation or support and maintenance.

Keeping a Stringent Selection Process

The channel partner market is crowded and fragmented. Once the ideal partner types are identified, the next step is to filter the pool of prospective partners. The secret to having a successful market entry through channel partnering is not through large numbers but in selecting strategically.

Working on the Right Chemistry

Channel partner engagement programs are 'a dime a dozen', but a good program creates a symbiotic relationship between the vendor and their partners allowing both to mutually benefit from the relationship in terms of topline, bottomline, market share and other strategic business goals.

Morphisec on Channel Partnering in India

Ajit Pillai

Regional Director - India/ SAARC at Morphisec

What are the different security channel partner models prevalent in India?

There are three different channel partner models which have evolved over a period of time. Initially if you take a step back, it was primarily a two-tier model which used to be a distributor and channel partner. That used to be the legacy. But it eventually moved into three different kinds of model.

1st Model - The traditional model–distributors who had a second layer of value-added resellers, system integrators, consultants and regional partners who did the sales.

> There are three different channel partner models which have evolved over a period of time.
> Ajit Pillai, MORPHISEC

2nd Model - Over a period of time, a lot of innovative technology started coming up which the regular distributors started losing to value-added distributors. This set of value-added distributors evolved to having a new set of partners other than traditional retail resellers. You had national system integrators and regional system integrators. A lot of new players came up who were focused exclusively on the products. This is the value-added model that is currently relevant for vendors selling Push technology- less demand from customers, wherein the OEM and channel partners need to position the tech and sell the same.

3rd Model - The third model is very disruptive primarily because it's a cloud adoption model. So, we have newer players who have come in who initially followed the MSSP trend but moved on to selling hybrid solutions- both products and services. Here also we have two sets of partners but at the end of the day they source the products from a distributor, the value-added cloud model got a new set of resellers/partners who actually followed the hybrid model. So, in that traditional partners and products like Microsoft or HP started off with services on top of their products by adding different tech like storage, AI, ML, analytics or DL.

For cyber security, in 30 years there have been 40 different innovations that have driven the market. The 40 are mainly divided into three - data security, endpoint security and network security.

What are the components of a successful channel partner strategy in India? What would be the ideal security channel structure? Would this structure be different for security hardware, software and service vendors? If yes, how?

For this we have to look into how the current market is behaving. It is all end-customer and technology driven - the two factors which drive sales.

Next we have to define the three segments:

- Enterprise
- Mid-market
- SMB

The major factor considered is the technology per se. In that there are two types, value-added tech and on-demand tech.

Currently there are multiple products/tech that could be put into multiple baskets. It's kind of a matrix – one side on the X axis we have the products and on the Y axis we have the market which is enterprise, mid market and SMB. Anything above 5,000 employees is categorized as enterprise, 1,000-5,000 employees is mid-market and less than 1,000 employees are SMB.

For cyber security, in 30 years there have been 40 different innovations that have driven the exercise. The 40 are mainly divided into three - data security, endpoint security and network security.

The strategies for each market differ. enterprise market is driven by compliance. Mid-market is driven by value-added services, SMB is driven by bundled services.

Customer demand evolves the channel strategy in India for cyber security. There is no set model. The model to be followed is set by the OEM, tech, consumers and the market.

What are the key partner characteristics you should look for while choosing a distributor, SI/VAR or reseller channel partner for a security brand?

We should look at multiple things while seeking a channel partner. We understand what our G2M strategy is, we know exactly which are the set of customers, which are the verticals we need to target etc. Based on the capabilities and the value addition the partners will be able to deliver in each of the markets we choose.

- Enterprise level- we look for the type of value add and track record
- Mid market level- we look for ability to shuffle costs to meet demand
- SMB level- we look for ability to bundle products/services and give additional service depth.

Other characteristics we look for are the infrastructure, network and motivation to reach targets.

What is the ideal strategy to engage and develop security channel partners in India?

There is no thumb rule to approach this. It's all dependent on understanding the tech and G2M. Any strategy should be market coverage from people who understand the tech and give value addition to customers based on segment. That means at enterprise it is about creating multiple, continuous sales; at mid-market it is about cost economics, and at SMB level it is about creating a perception so that customers are comfortable with buying the solutions.

MORPHISEC
Moving Target Defense

Dayanand Muthukrishnan

Code Red Security PR Network

FORTINET®

Fortinet was founded in 2000 by Ken Xie, the visionary founder, former president and CEO of NetScreen, later sold to Juniper for more than $3.5 billion. Headquartered in Sunnyvale, California, Fortinet had customer support, development and sales facilities throughout North America, Europe and Asia to ensure continuous customer success.

Fortinet pioneered the concept of Unified Threat Management (UTM) solutions. At the heart of this solution were the company's award-winning FortiGate™ series of ASIC-accelerated Antivirus Firewalls, the new generation of real-time network protection systems that helped detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time — without degrading network performance.

The FortiGate systems delivered a full range of network-level services — stateful firewall, SSL and IPSec VPN, intrusion prevention and traffic shaping — as well as application-level services such as antivirus and web content filtering, in dedicated, easily managed platforms.

Situation:

- Fortinet had just entered the Indian market where enterprise customers followed the practice of maintaining disparate security devices or point security solutions and were unaware of ASIC accelerated Unified Threat Management appliances. pioneered by the company and significant benefits these offered in protecting the enterprise from newer generation of content based threat vectors.
- IT administrators strongly believed that consolidating multiple security capabilities like URL filtering, anti-virus scanning, spam-filtering, firewall, into one centrally managed solution would degrade not just security effectiveness but also end user application experience

- Following the initial success of UTM appliances in the SMB market most enterprise IT managers were convinced the company would not be able to scale appliance functionalities to serve the high I/O and OLTP needs of enterprise IT environments
- Security product purchases were predominantly driven by SI/VAR recommendations at the enterprise level. To succeed, Fortinet had to carefully cultivate a loyal base of channel partners who would not only educate key customer segments but also help position the UTMs into available enterprise network and application environments

PR Goals:

- To create broader awareness about UTMs and advantages of deploying ASIC-accelerated unified threat management appliances and their effectiveness in combating multi-vector threats from both within and outside the enterprise without any degradation of performance in terms of speed or effectiveness
- To showcase success of Fortinet UTM solutions across SMB and mid-market enterprise segments to be able to establish stronger presence in large enterprise and carrier class IT environments
- To create an image for Fortinet as a company with a special focus on the Indian market and whose products and services are highly relevant for the evolving Indian business situation

Strategy:

- Implement an aggressive PR program centered on high-impact editorial coverage by reaching to tier-one trade, mainstream, business and industry vertical press
- Educate key media editors, technology analysts as to the success of ASIC accelerated Unified Threat Management **solutions in markets similar to India using Fortinet's pioneering** position to validate the company's continuing leadership in this space
- Educate target customers and channel partners continuously and across consumption points by bringing into focus numerous story threads including the evolving threat landscape due to rising broadband/mobile/BYOD penetration; demonstrating value propositions offered by Fortinet solutions across customer pain points and use cases.
- Execute a consistent PR program to ensure momentum remains intact throughout the year

Results delivered:

- Within 12 months of launch, Fortinet dominated bulk of security stories across trade, mainstream and business outlets; constantly showcasing every powerful aspect of its path breaking UTM solutions and its relevance in the evolving threat landscape. In fact, Fortinet was the preferred media port of call for anything to do with evolving threat landscape and, of course, UTMs in India
- Media and analysts were continuously engaged, and the company was rewarded with strong media mindshare and positive recommendations
- The PR campaign, at the heart of the company's marketing initiatives for the first 24 months, helped catapult a relatively emerging security segment like UTMs into mainstream discussions through a combination of structured storytelling and strong band championing both at the EXL PR and client side
- Fortinet received numerous awards from trade and business media for its strong entry and leadership role in the rapidly growing UTM market in India
- There was consistent, high level visibility for key Fortinet leadership, both for in-country and visiting executives, across print and broadcast media

Dayanand Muthukrishnan

Code Red Security PR Network

For over 35 years, Futurex has been a globally recognized provider of hardened, enterprise-class data security solutions. Over 15,000 customers worldwide have trusted Futurex's innovative Hardened Enterprise Security Platform and the VirtuCrypt Hardened Enterprise Security Cloud to provide market-leading solutions for the secure encryption, storage, transmission, and certification of sensitive data.

The Hardened Enterprise Security Platform is a collection of advanced data security solutions that operate together to produce a result far beyond the sum of its parts. Trusted by Tier 1 organizations worldwide, the platform offers scalability, versatility and security to provide a secure and comprehensive protection

Situation:

- Futurex was preparing to open their second international office in India to support of the region's rapidly expanding needs for enterprise cryptographic hardware and cloud-based services
- Under the leadership of industry expert Ganesh Karri, Chief Solutions Architect and Regional Business Manager for South Asia, Futurex planned to expand their presence in the region by working directly with customers as well as supporting a select network of highly qualified Tier 1 channel partners
- To establish a strong presence in a burgeoning market, Futurex reached out to EXL PR to help cultivate strong brand awareness and connect for its solutions in India

PR Goals:

- To create brand visibility and establish strong media presence
- To create broader awareness about cryptography based security platform and cloud solutions and the advantages of deploying such a comprehensive solution to secure every aspect and endpoint of organizations' core cryptographic infrastructures, from key management to data encryption to secure storage
- To showcase effectiveness of Futurex Hardened Enterprise Security Platform and the VirtuCrypt Hardened Enterprise Security Cloud solutions across SMB and mid-market enterprise segments to enable stronger penetration in large enterprise and carrier class IT environments
- To create an image for Futurex as a company with a special focus on the Indian market and whose products and services are highly relevant for evolving Indian businesses

Strategy:

- To introduce the Futurex brand to the Indian market through targeted media briefings, press releases and exclusive leadership interviews
- Implement an aggressive PR program centered on high-impact editorial coverage by reaching out to tier-one trade, mainstream, business and industry verticals press
- Educate key media editors and technology analysts as to the dynamics of Futurex Hardened Enterprise Security Platform and the VirtuCrypt Hardened Enterprise Security Cloud solutions and its advantages over other similarly placed solutions
- Execute a consistent PR program to ensure momentum remains intact throughout the year

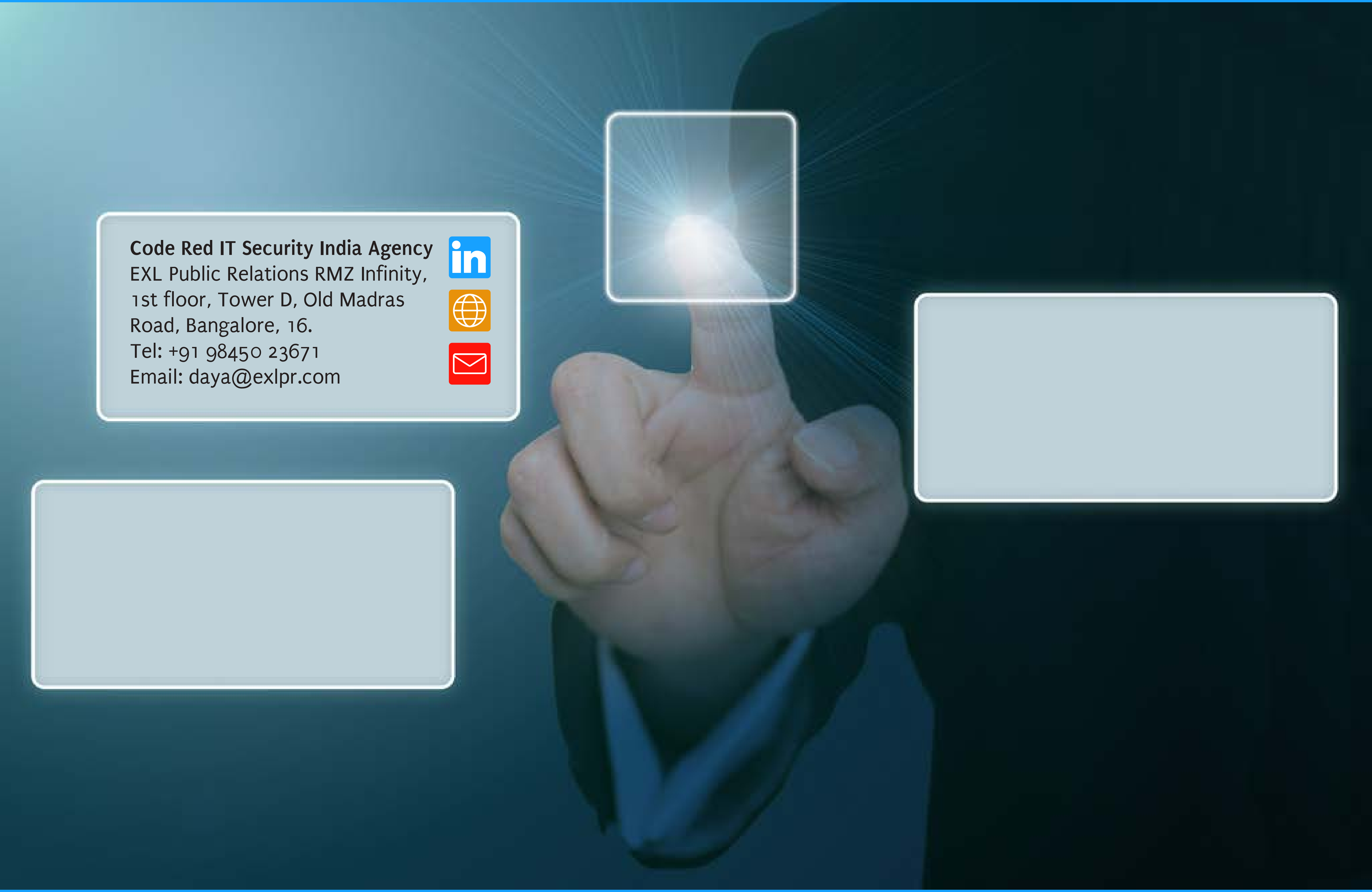
Results delivered:

- Through an aggressive PR campaign and strong brand championing, EXL PR successfully introduced Futurex to India.
- Media and analysts were continuously engaged, and the company was rewarded with strong media mindshare and positive recommendations.
- Consistent, high-level visibility for Futurex leadership and its solutions, was achieved across tier 1 media outlets.

Impact achieved through PR program:

Strong, consistent and positive PR campaign has helped Futurex launch their first office in India and expand their growing presence in the South Asian market.

Contact us



Code Red IT Security India Agency
EXL Public Relations RMZ Infinity,
1st floor, Tower D, Old Madras
Road, Bangalore, 16.
Tel: +91 98450 23671
Email: daya@exlpr.com