FROST & SULLIVAN

Advanced Recognition Systems: The New Paradigm in Asia-Pacific

A Frost & Sullivan White Paper

Sponsored by

NEC

Setting the Context: Evolution of Advanced Recognition Systems

Unlocking Transformative Social Value

Confluence of the Physical and Cyber Realms

Evolution of Big Data and AI within Smarter Cities

Explosive Growth of IoT Devices Globally

The disruptive trends mentioned above have led to the emergence of millions of digital natives who demand cutting-edge technology and innovative services with pervasive connectivity anytime, anywhere. Against this backdrop, Advanced Recognition Systems are becoming increasingly widespread with the growing implementation of biometric security in a number of sectors, particularly in banking, retail, law enforcement and border control.

According to a recent announcement by Tractica, the global biometrics market is forecast to grow to US$15.1 billion by 2025, at a 10-year CAGR of 22.9%. Asia-Pacific is anticipated to be the fastest growing market, owing to a surge in government biometric projects such as the e-passport and e-visa programs and heightened demand for advanced security solutions to combat rising crime, fraud, data theft, terror attacks and cyber-attacks.

This paper centres on how advanced recognition systems can become a gateway to digital and smart empowerment for future societies as seen through the lens of both governments and private enterprises.

Going Beyond Biometrics

Advanced recognition systems deliver more than just conventional biometric functions. For starters, biometric entails unique characteristic of an individual, be it physiological or behavioural traits to verify a person's identity. Physiological biometrics extends to the use of physical features such as a person's face, iris, fingerprint, palm and DNA, whereas behavioural biometrics measures a person's patterns, such as gait, voice, and handwriting.

While behavioural biometrics has yet to mature, a large portion of biometric systems involve automated biometric identification system (ABIS), widely used by law enforcement agencies worldwide to identify criminals or persons of interest. The Federal Bureau of Investigation (FBI), for instance, has established the world's largest biometric repository for law enforcement, housing over 70 million subjects' fingerprint records in its Criminal master file, and 31 million civilian fingerprints. Recent upgrades to this system have significantly improved the turnaround time to identify a subject – from 48 hours to less than just 2 hours – enabling law enforcement to execute swift and immediate response to aid criminal and forensic investigations.

Biometrics is also being progressively used for identification and access control in various industries due to its security, efficiency, and convenience features. Unlike traditional authorisation methods, such as PINs and passwords, biometrics cannot be lost, forgotten, exchanged, and is very difficult to forged making it the preferred approach for personal identification. While this indicates the potential for biometrics to soon become the global standard for access control, simple physical verification alone is not enough.

Data breaches are a common phenomenon today, given the enormous amounts of data being exchanged daily and blurring boundaries between physical and cyber spaces. With the rise of cloud, social and mobility, a person no longer has a single physical identity but multiple identities across applications, devices, and objects. The Global Breach Level Index, for example, recorded 918 data breaches worldwide in the first half of 2017 – representing a 13% increase from the year before – of which 47 incidents occurred in Asia-Pacific, including 15 in Australia.

The most recent Equifax debacle, reported to have affected nearly 146 million Americans, is another grave reminder of the importance of robust security for data-dependent business operations. Needless to say, the security landscape has grown so complex that service providers are now forced to develop more stringent security measures. The future of public safety will be determined by secure digital identity that sets itself apart with efficiency, convenience, and customer experience.

Although biometrics enforces a more sophisticated level of security, no single security platform is infallible. Each has its own advantages and disadvantages in terms of ease of capture, accuracy, performance and cost. In moving beyond biometric authentication, advanced recognition systems can provide next-generation integrated security solutions, and create an ecosystem to enhance safety, intelligence and performance of organisations and society.

Three-pronged Approach to Advanced Recognition Systems

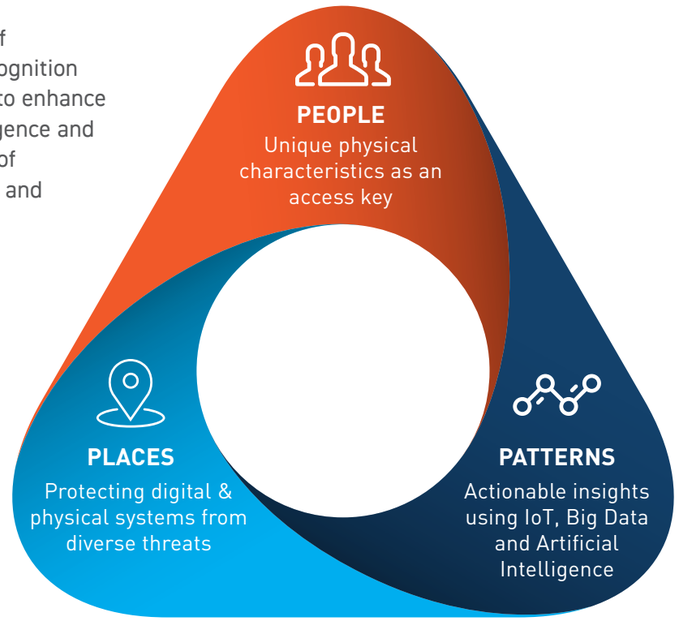
People. Places. Patterns

Advanced recognition systems today represent the new frontier of growth and security supported by the 3Ps: People, Places and Patterns. This three-pronged approach introduces a more multifaceted system beyond the conventional form of biometrics.

People – From Unimodal to Multimodal

The concept of advanced recognition systems underscores the need for multimodal biometrics in overcoming the limitations of individual biometrics, also known as unimodal biometrics. The reliability and accuracy of unimodal biometric systems may be compromised by factors such as the presence of noisy data, lack of invariant representation, and spoofing. Usage of a single biometric modality may be susceptible to producing "erroneous results"; for instance, the accuracy of facial recognition technology could be challenged by poor lighting conditions and resolution images or when identifying individuals bearing similar facial features.

Ecosystems of advanced recognition technologies to enhance safety, intelligence and performance of organisations and society



Adding biometrics to a physical security factor (like password or swipe card) to form a 'Multi-factor Authentication' process can provide some improvement. However, to fully overcome the threat, multimodal biometrics is the way to go forward. Multimodal biometrics employs a fusion of biometric information (i.e., two or more biometric modalities) for improved performance of recognition results (e.g., reduced false acceptance rate), and increase the robustness of security systems. Research has shown that a combination of face, fingerprint, and iris methods during the enrolment, verification or identification process provides accuracy of up to 99.5%.

3Ps	Key Technologies*	Application*
PEOPLE	• Fingerprint Identification • Facial Recognition • Voice Recognition • Iris Recognition • Palm/Vein Recognition • Multi-Biometrics • Mobile Identification Software • Liveliness Detection	• Border Security • Law Enforcement • Financial Services • Retail • Industrial
PLACES	• Advanced Security Surveillance • Cybersecurity • Information Security	• Border Security • Law Enforcement • e-Government • Financial Services • e-Commerce • Retail • Industrial
PATTERNS	• Crowd Behaviour Analysis • Behaviour Detection • Meta-Analysis • Object Recognition • Rapid Machine Learning • Invariant Analysis • Textural Entailment • Heterogeneous Mixture Learning • Voice/Sound Analytics • Congestion Prediction	• Law Enforcement • e-Government • Financial Services • e-Commerce • Retail

** Non-exhaustive list*

Places – From Physical to Cyber Spaces

The current scale of terror attacks and cyber threats is unprecedented. From the Las Vegas massacre – the deadliest yet in US history – that claimed more than 50 lives and injured over 500, the London tube bombing attempt that left 30 people injured escalating UK's terror threat level to "Critical" to the WannaCry ransomware that crippled over 300,000 computer systems at global businesses, the list continues to grow.

The estimated cost of global terror attacks hit US$90 billion in 2015, with Asia-Pacific accounting for 7% of all attacks and 2% of deaths, according to the Institute for Economics and Peace. Frost & Sullivan research suggests that cyberattacks targeting critical infrastructures, on average, cost organisations between US$3 million and US$12+ million per year. Protecting digital and physical systems from diverse threats is no longer a consideration, but a top priority for global businesses. Such attacks can be curbed through effective deployment of video surveillance systems and cybersecurity mechanisms.

Patterns – From Analytics to Predictions

Although biometrics is strengthening the level of security significantly, however, in its current state, this authentication technology still faces challenges in successfully mitigating terrorist activities and digital-based financial crimes.

Extensive research and development efforts to address this issue have led to the integration of biometric technology, such as facial recognition, with Artificial Intelligence (AI) to be used in video surveillance systems. Sophisticated software algorithms can effectively detect and prevent suspicious activities to counter cyber-physical threats in the community – improving security tremendously. AI-based biometric solutions are forecast to gain greater adoption as a method of authentication in high-density public areas such as shopping malls, airports, railways, and classified zones.

Voice biometrics can also be embedded with AI, which is an increasingly common digitisation approach in the banking and telecommunication sectors. AI-based voice biometrics could even facilitate direct communication with chatbots up to the emotional level of understanding. In short, the integration of AI and biometric technology demonstrates enormous potential for mass surveillance and remote authentication applications in the public and commercial sectors respectively.

The Next Smart Deployment Model

The three-pronged approach – People, Places and Patterns – complements one other. Advanced recognition systems leverage a combination of physical and cyber security platforms, reinforced by data analytics and AI. By integrating the People, Places and Patterns components, a total solution can be delivered in multiple industries, one that is versatile, scalable, and flexible.

No longer a separate technological component, advanced recognition systems can be seamlessly incorporated into everyday lives, going beyond simple security. By the end of 2017 Frost & Sullivan estimates 8.4 billion connected devices to be installed worldwide; approximately 37% of the devices will be used by businesses with the remaining by consumers. By 2020, the figure is expected to surge to more 20 billion connected devices. As the use of biometrics extends into broader commercial applications, the three-pronged approach may become the very fabric of future smart ecosystems.

As such, tech-savvy users could become more accustomed to advanced recognition systems to carry out the simplest of tasks, such as making digital P2P payments with fingerprints or passing through immigration using borderless gates in a matter of seconds. Not only that, advanced recognition systems, when integrated to commercial services, often provides twofold benefits - an increased level of security as well as improved speed and/or convenience for consumers. Subsequently, business models could be built upon such systems to enable a more sustainable and robust approach to connecting with consumers through personalised experiences, significantly driving the quality of life.

Emergence of Advanced Recognition Systems in Asia-Pacific

Bringing a Futuristic Perception of Australia

Australia is riding on the wave of deploying contactless technologies as the government invests millions into biometric solutions to build a strong foundation for advanced recognition systems in the region. Meanwhile, the commercialisation of biometrics technology continues to deliver frictionless customer experience in various industries, particularly in banking and retail.

A GOVERNMENT PERSPECTIVE

BORDER SECURITY

ePassports, eVISA, eGate (Automated Border Control gates)

LAW ENFORCEMENT

ABIS, Live Scan, Mobile ID

E-GOVERNMENT

National ID, Health cards, Driver's Licence, Welfare cards

Seamless Traveller Initiative in Australia

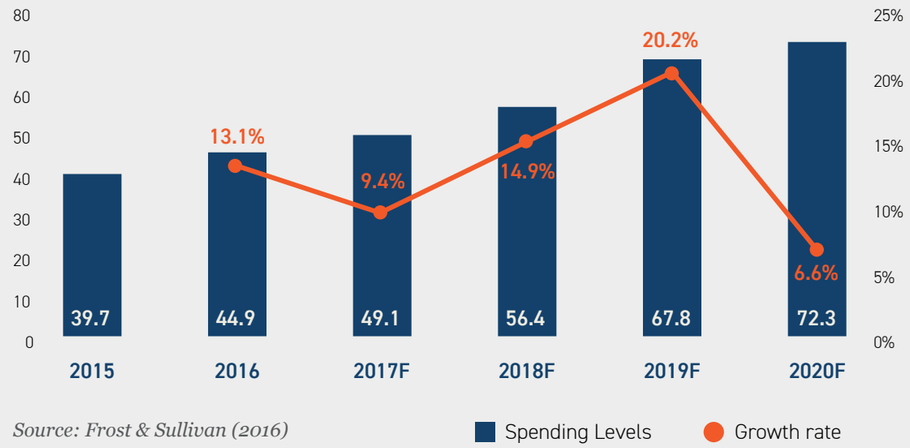
PEOPLE

The biometric-enabled passenger process is reshaping travel experiences and increasing in prevalence in many Asia-Pacific countries – and Australia is no exception.

With the launch of the **A$100 million Seamless Traveller Initiative**, the Department of Immigration and Border Protection (DIBP) envisions a 2020 target of automating 90% of border clearance processes through multiple biometric systems – fingerprint, iris and facial recognition – to go completely "contactless". The unique traits of biometric systems present greater security and accuracy when verifying a traveller's identity compared to physical passports which can be easily lost, stolen or forged.

In early 2017, the DIBP scrapped and replaced outgoing passenger cards (OPCs) with biometric scanners, and incoming passenger cards (IPCs) are expected to follow suit. Brisbane Airport is already leading trials with facial recognition services from check-in to boarding. Passengers can expect the roll-out of facial recognition systems at all airports in Australia to be completed by 2019.

Automated Border Control Market Forecast, US$ Million, Asia-Pacific, 2015–2020F



Source: Frost & Sullivan (2016)

According to Frost and Sullivan research, Australia accounted for 52.8% of spending in the Asia-Pacific Automated Border Control (ABC) market in 2015. For example, the Australian Federal Police and Department of Foreign Affairs and Trade implemented the Face Verification Service (FVS) in 2016, as part of its efforts to reduce cross-border criminal activities by allowing law enforcement agencies to share citizens' facial images to verify identities and identify unknown individuals. The delivery of such biometric solutions is set to "transform border experience" as the DIBP anticipates annual passenger traffic to grow to 50 million by 2020. As travel to and from Australia gets easier, this is likely to lead to more cuts to red tape, further promoting the tourism industry in the country.

Cybersecurity Strategy in Australia

PLACES

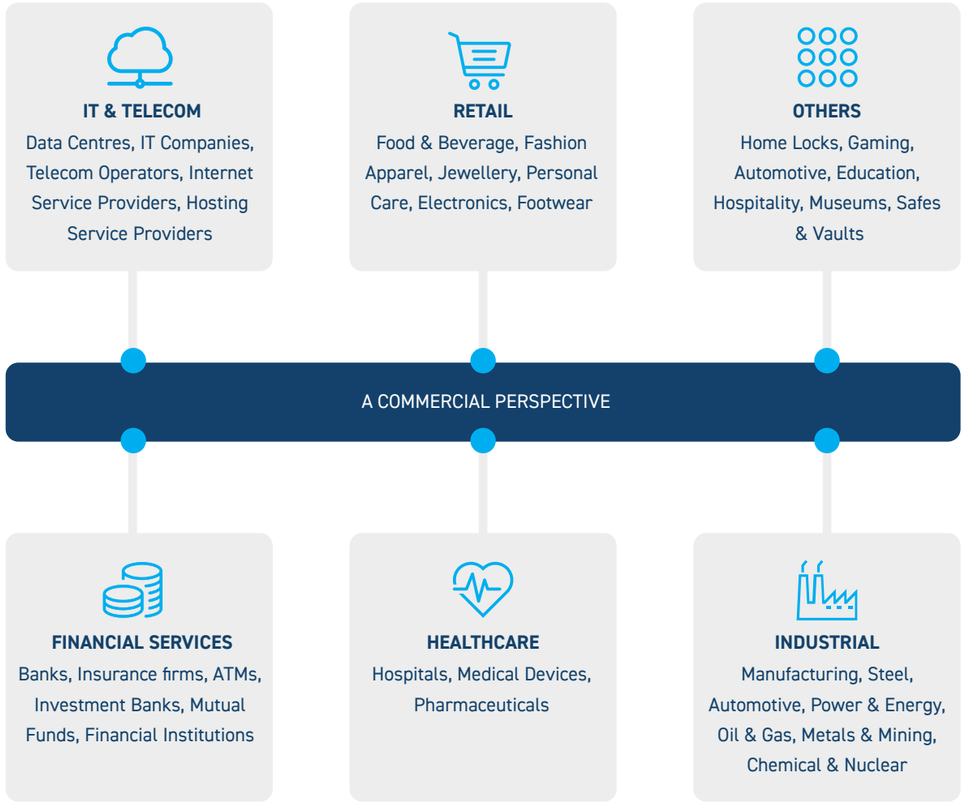
Disruptive business models and the technologies that enable them, such as Big Data Analytics, IoT and mobile Internet, are expected to garner incremental annual economic value of US$625 billion by 2030, constituting 12% of Asia-Pacific's total projected GDP[1]. As Australia becomes more digitally connected, stronger cybersecurity measures remain pivotal in securing long-term economic growth and prosperity.

Australia has long been a prime target for malicious attacks as organisations in the country reportedly experienced cybercrime at double the global rate in 2016. A major phishing attack against the Brisbane City Council in August 2016 demonstrated just how easily security systems can be threatened. The council lost A$450,000 of taxpayers' money to a scam account set up with fake invoices and email addresses. The Australian Bureau of Statistics (ABS) also faced a Distributed Denial of Service (DDoS) attack in 2016 when millions of Australians were blocked from completing the online survey for the eCensus.

Recognising the dynamic opportunities digitisation presents, Australia unveiled its very first Cyber Security Strategy in mid-2016 to strengthen the local cybersecurity industry as one of its five priority actions. Despite developing a highly-publicised four-year strategy, Australia has made little progress in building a strong cybersecurity infrastructure. As of May 2017, the A$230 million Cyber Security Strategy has only realised four out of its 83 initiatives; it is no surprise then that the country continues to lag behind in the Global Cybersecurity Index (GCI). In 2017, Australia's ranking dropped four places, down to the seventh spot, treading behind regional peers Singapore and Malaysia.

That stated, Australia's cyber defence potential remains strong as the ACSGN[2] estimates the local cybersecurity industry to grow threefold to A$6 billion by 2026 from A$2 billion today, backed by the active government support indicated in the 2017 Cyber Security Sector Competitiveness Plan (SCP).

[1] Australia Cyber Security Strategy
[2] Australian Cyber Security Growth Network

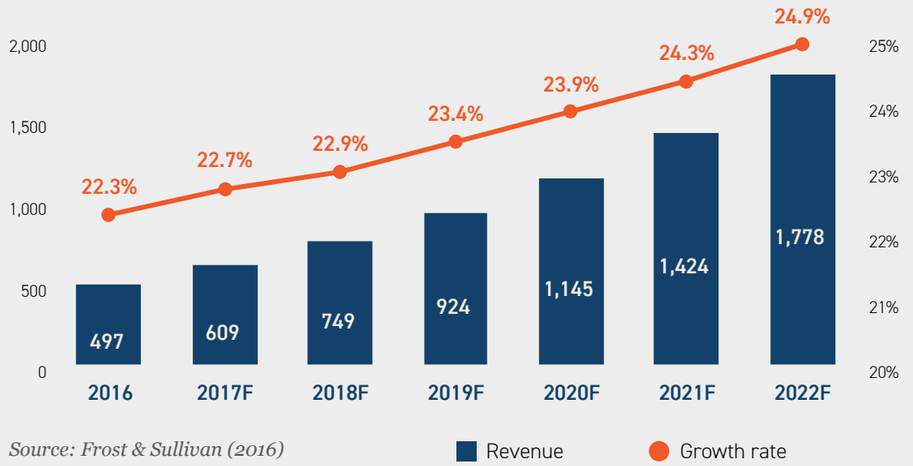


Bringing Frictionless Customer Experience

The proliferation of advanced recognition systems in financial services has become inevitable as the industry shifts into employing more robust and secure authentication processes. Biometrics is empowering banks and financial institutions to not only improve their KYC and AML processes, but also reduce the time taken to conduct banking transactions, increase customer satisfaction levels, and safeguard their interests.

Protecting customers' banking information and creating a secure, seamless mobile banking experience is one of the biggest drivers behind adoption of biometrics in banking. Remarkably, the APCA Fraud Statistics[3] suggests that fraudulent activity in Australia recorded a 93% hike from 2013 to 2016 with customers losing up to A$534 million to fraudsters in 2016; 78% of all fraud on Australian cards over the period was carried out using stolen credit card details. As the payments landscape goes digital, fraudsters are also employing malware and phishing attacks to steal sensitive card data, even going as far as bypassing fraud detection systems.

Total Biometrics Market in Banking, US$ Million, Asia-Pacific, 2016–2022F



Source: Frost & Sullivan (2016)

In response to such widespread concerns, Citibank became the first bank in Asia-Pacific to deploy voice biometrics technology with more than one million sign-ups in its 2016 launch year. In a recent media release, the bank indicated how the move has cut the time required to authenticate customers by two-thirds, from 45 seconds to under 15 seconds.

[3] Australian Payments Clearing Association

Amid the growing trend of mobile biometrics, it is becoming more sustainable for banks to deploy advanced recognition systems as a means for better security resilience, cost savings, and seamless customer experience. Visa's latest move to push Australian banks to go PIN-less with biometrically-authenticated transactions and ANZ's new voice biometric authentication process at its call centres, support this trend.

The alarming increase in online fraud sweeping the digital payments landscape requires banks to adopt effective mitigation strategies. Advanced recognition systems, in this regard, can pave the way for compliance with the Payment Card Industry Data Security Standard (PCI DSS) in strengthening data security.

The use of biometrics **(from the people aspect)** can bring advanced authentication methods

The implementation of video surveillance and cybersecurity tools **(from the places aspect)** can protect sensitive information from data breaches

The use of advanced analytics **(from the patterns aspect)** can predict fraud behaviour and prevent financial crime in real-time

With retailers going omnichannel through brick and mortar stores and e-commerce platforms such as Amazon and TaoBao, advanced recognition systems can unveil new opportunities for retail businesses. The ever-changing buying patterns of tech-savvy customers are propelling the need for customer analytics gathered through means of video and cyber surveillance technology. In addition, intelligent surveillance solutions can bring actionable market insights and customer intelligence from crowd behaviour to heat map data.

Undoubtedly, demand for advance surveillance systems and video analytics has soared due to the fact that security concerns consistently top the priority list of many private enterprises. Convenience store chain, 7-Eleven, recently signed a deal with Fair Work Ombudsman (FWO) in Australia to deploy biometric scanning systems and CCTV cameras to prevent unlawful workplace practices. Meanwhile, the Parliament of New South Wales is exploring the feasibility of CCTV implementation to protect school children from potential abuse and neglect, and improve classroom teaching and management practices.

As commercial sectors, such as banking and retail, progressively embrace advanced recognition systems, lack of proper infrastructure and high implementation costs may hamper adoption levels. Even though the security and productivity offered by biometric technologies far outweigh the cost factor, the extent of implementation remains at the discretion of organisations. Australian enterprises should put more focus to align the needs of customers and rising development of advanced recognition systems as a competitive advantage to create a consistent, seamless customer journey.

Advanced Recognition Systems can, thus, transform the experience of customers, employees, and bring a higher level of efficiency by enabling new applications and innovative digital services in public safety context.

The Last Words

NEC Pioneering Advanced Recognition System in Australia

As Australia becomes more connected, government services and private enterprises are increasingly more vulnerable to physical and cyber threats as highlighted in the previous sections. Of late, decision-makers have to come to terms that preventive and proactive measures need to be taken to safeguard the assets that are critical to their business. It is, therefore, important for business leaders and key influencers to appoint an established technology partner with a proven track record in Australia and the foresight to anticipate threats that may not exist today.

NEC Australia is investing substantially in technological innovations to safeguard against integrated cyber-physical attacks using the industry-leading three-pronged approach (People, Places and Patterns). It has been commissioned by a number of government authorities in Australia to deploy a comprehensive suite of advanced recognition systems that includes biometrics and video analytics that visualise human behaviour, detect wanted individuals, safeguard restricted premises, and translate data into insights in real-time to support informed decisions.

Recent examples include a five-year contract to deliver nationwide multi-modal Biometric Identification Services (BIS) for Australian Criminal Intelligence Commission (ACIC), formerly CrimTrac. Furthermore, NEC Australia is supporting the forensic, investigative, and front-line policing operations of South Australia Police (SAPOL) that features its internationally acclaimed NeoFace® facial recognition software. The Northern Territory (NT) Police Force in Australia is also in the process of implementing NEC's leading edge forensic facial recognition technology to fight crime and keep communities safer.

As the undisputed pioneer in multimodal biometrics authentication with substantial advances in terms of accuracy, NEC's Advanced Recognition Systems apply some of the most cutting-edge technologies in the world. The company has carried out large-scale deployments in border automation, e-passports, law enforcement identification, crowd control, and citizen surveillance in a growing number of Asia-Pacific countries. Recognising its wide and diverse range of product portfolio and more than 40 years' local experience, Frost & Sullivan awarded NEC Australia the prestigious Australia Biometrics Vendor of the Year award in 2016.

NEC remains firmly at the forefront of superior technical expertise, strategic partnerships, and compelling thought leadership, supporting government authorities and business entities to accurately anticipate when, where, and the extent of the next possible attack.

We Accelerate Growth

WWW.FROST.COM

Auckland	Colombo	London	Paris	Singapore
Bahrain	Detroit	Manhattan	Pune	Sophia Antipolis
Bangkok	Dubai	Mexico City	Rockville Centre	Sydney
Beijing	Frankfurt	Miami	San Antonio	Taipei
Bengaluru	Iskandar, Johor Bahru	Milan	Sao Paulo	Tel Aviv
Bogota	Istanbul	Mumbai	Seoul	Tokyo
Buenos Aires	Jakarta	Moscow	Shanghai	Toronto
Cape Town	Kolkata	New Delhi	Shenzhen	Warsaw
Chennai	Kuala Lumpur	Oxford	Silicon Valley	Washington D.C.

ABOUT FROST & SULLIVAN

Frost & Sullivan is a growth partnership company focused on helping our clients achieve transformational growth as they are impacted by an economic environment dominated by accelerating change, driven by disruptive technologies, mega trends, and new business models. The research practice conducts monitoring and analyzing technical, economic, mega trends, competitive, customer, best practices and emerging markets research into one system which supports the entire "growth cycle", which enables clients to have a complete picture of their industry, as well as how all other industries are impacted by these factors.

Contact us: Start the discussion

To join our Growth Partnership, please visit www.frost.com

ABOUT NEC

NEC Corporation is a leader in the integration of IT and network technologies with a presence in 160 countries and $25 billion in revenues. NEC delivers integrated Solutions for Society that are aligned with our customers' priorities to create new value for people, businesses and society, with a special focus on safety, security and efficiency.

For more information, visit NEC at www.nec.com