DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE IN SECURITY

Digital Transformation and emerging technologies driving security opportunities across industry sectors

LEARN MORE
For more information on the digital transformation and emerging technologies

www.isnrabudhabi.com
INTRODUCTION

We live in one of the safest times in history, however, unresolved conflicts and evolving threats continue to have a significant impact on governments, business, and people. At a national level investment in security still remains a critical priority for governments across the world. Frost & Sullivan's analysis of the major security markets shows expenditure on security technology by public safety organisations and critical infrastructure operators is forecast to be $158.4 Billion in 2018. This is expected to continue to grow at just over 5% until at least 2022.

Demand and growth are driven by traditional factors that include:

Chart 1: Drivers of Security Investment

In addition to these factors the security landscape is changing through the digital transformation of society and evolution of technology. It is fuelled by increasing digitisation (for example, the number of mobile devices), connectivity (the ability to connect devices, people and processes), and data. Many critical infrastructure industries are going through a digital upgrade to improve operational efficiencies, customer satisfaction, and to create new services. This is having a significant impact on driving new security systems and solutions.

One of the major changes is convergence of data and the push towards increasingly high levels of integration between traditionally disparate security systems. This in greater availability of security and operational insight for security stakeholders facilitated by both the growth of increasingly smart technology and sensors together with massive strides in IT, data analytics and software capabilities. This, combined with increasing system intelligence and pre-emptive capabilities, makes the modern security system more responsive, effective and adaptive to security threats.
In the past, the slow moving and cautious nature of the security market and preference for tried and tested equipment hindered wide spread adoption of new technologies. Many security operators took a more reserved approach, and waited to see results and benefits of early adopters. This was understandable because security and technology cannot fail in their operating environments. However, over the last few years we have seen the maturity of technology and proof of concepts which has resulted in numerous programmes and investments across the world to upgrade and replace existing security systems with digital, data driven solutions.

Moving forward there will be greater adoption of emerging technologies by public safety agencies and security end users across industries. The technologies provide clear benefits in operational efficiency and situational awareness. They can significantly aid a security operation to provide better protection whilst often providing costs savings. As these are further proven in the commercial environment, we will see increasing investments from security end users. The table below outlines the expected timelines for some of the technologies that will have the greatest impact on the security market.
The UAE, and specifically Dubai police force has been one of the early adopters of new security technology. This has been possible due to greater budget availability, fewer issues of legacy equipment and backing from key government stakeholders. It has been a clear and stated aim to build one of the most technologically advanced police forces in the world. Investments in strategic technology programmes have delivered solutions that have enabled them to anticipate and provide a quicker response to events and threats to better protect citizens and visitors across the city. The recent announcement of the Dubai police strategic plan to 2031 confirms this commitment to invest in new technologies and ensure they will have the latest security systems and solutions for their officers. The chart below captures some of the announced programmes, contracts and partnerships that have been the foundation of their digital journey.
THE DEVELOPING ROLE OF AI IN SECURITY

One of the key technologies that will significantly impact the security market is Artificial Intelligence. There are numerous benefits and applications to security end users, and there are already a number of case studies in the market. Improvements, both in terms of computer processing power, sensor interconnectivity and the technical infrastructure of security end users, have seen the intelligence of security systems improve dramatically over the last 5 years. Moving beyond simple demonstrations of smart video camera capabilities, early machine learning and artificial intelligence capabilities are poised to revolutionise how we interact with security processes and more importantly, how they can be more pro-active to our needs. Whilst adoption of these systems remains relatively low, improvements around reliability, performance and most importantly costs have seen discussions around AI as a security tool evolve rapidly. The chart below outlines the key applications of AI in security.

**Chart 5: AI Applications in Security**

The necessity for more intelligent and automated systems, with the long-term vision of AI, is born of the need to manage large volume of data being delivered as part of the modern security setup. Whilst networking of systems and sensors can deliver rich, contextual knowledge to customers, an inability to interact with this information in a timely fashion diminishes its value. At its core, smart systems and AI allow organisations to scale up insight without the need to scale up manpower.
The role of smarter AI systems in developing cyber security offerings and solutions has been essential in helping organisations streamline their responsiveness to digital threats. This same application of more intelligent technology is also making its way into the law enforcement space, with examples of technology intelligence functions being tasked with complex video analysis, pre-emptive crime analysis and enabling officers to engage with systems by using voice and gesture commands.

The challenge for the industry, however, is proving that these systems can make consistently smart and correct decisions, based on a broad range of threats. Whilst systems are undoubtedly getting smarter, their ability to decide on their own course of action and learn from previous experience is currently still lacking.

Despite these challenges, AI will be an important part of security systems over the next 10 years. Numerous security suppliers have started to advertise this and put AI at the core of their offerings, with further competitors expected to follow suit.

**CONCLUSION**

The dynamics in the security market will continue to evolve. Hanging threat landscapes and digital transformation and new technologies will change the operational environments for security. This will drive demand for more advanced security systems.

The role of the industry in helping to guide and shape these increasing customer needs has never been more important, forcing suppliers to become more pro-active in delivering systems and concepts instead of just technology and standalone solutions. New solutions and technologies must address operational issues, increase security or provide significant cost efficiencies for end users if they are to be successful in the market. The security market will continue to grow with further investment from end users providing a range of opportunities for industry. Successful companies will adapt their solutions to the market changes and focus on solving customer problems.
Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding Frost & Sullivan's whitepaper, please write to:

ANTHONY LEATHER
Principal Security Consultant, Aerospace, Defense & Security - Frost & Sullivan
E : anthony.leather@frost.com
P : +44 (0)208 996 8517

DIOGENIS PAPIOMYTIS
Director, Aerospace, Defense & Security - Frost & Sullivan
E : diogenisp@frost.com
P : +971 (0) 443 318 82

ANITA CHANDHOKE
Corporate Communications - Frost & Sullivan
E : achandhoke@frost.com

www.isnrbudhabi.com | www.frost.com