



# Paving the way for a new era of cognitive security and surveillance







# Foreword

Physical security is at the heart of any leading global city's aspiration. Today, it is enabled through cutting-edge security systems which aim to prevent incidents and keep citizens and critical infrastructure safe.

This paper sets out to profile and analyse the current security landscape in the Middle East, with respect to its stakeholders, emerging technologies, opportunities, challenges and implementation strategies. Our aim is to define key drivers and evaluate partnership models that will help governments and security agencies to create highly individualised yet scalable solutions.

We are grateful to the participating domain experts for their valuable time, and for sharing their thoughts and points of view with us.

PwC is excited to collaborate as knowledge partners with Intersec, and to share our insights and point of view on the evolving physical security ecosystem in MENA. We hope you find this report insightful and useful and look forward to your feedback.



## Rajat Chowdhary

Partner, Technology  
PwC Middle East

Scan to view  
the introduction  
to the paper



# Table of contents



## Introduction

04



## Defining the stakeholder ecosystem

Introducing SS-ECO

05



## Changing landscape

Evolving customer needs

08



## Potential use-cases

Futuristic yet real

10



## Adapting to the cognitive wave

Activating CSS-ECO

12



## Customer-focused strategy

Re-alignment of approach

14



## Levers of shift

Accelerate innovation through partnerships

16



## Conclusion

18



## How can PwC help you achieve your goals?

19



# Introduction

Until recently the security and surveillance ecosystem had only a few stakeholder participants in product design and development. Yet as the ecosystem has evolved, more stakeholders are becoming active contributors. As innovation by OEMs (Original Equipment Manufacturers) has accelerated, user requirements have moved to the centre of this ecosystem and customers themselves are now playing a key role in shaping the industry.

The background to this change is one of the challenges related to adoption and implementation. Customers have been facing issues such as ecosystem interaction complexities and reactive modes of adoption. These challenges give rise to customised requirements and these too have been evolving. In order to address these requirements, the success factors include stakeholder collaboration, localised products and innovation in product and ecosystem DNA. This is the only way to meet the individual needs of the customer, using globally proven and locally relevant solutions.

Customers are already playing a much more active role, from product conceptualisation, to design and development, and also in commissioning. This shift is already apparent in the Middle East region and global disruptive use cases facilitated by technology-led innovation are now on the horizon.

Accordingly this paper focuses on defining the key drivers for adopting cognitive and contextual use cases through innovative customer-industry partnership models. It also provides an insight into how emerging technologies such as artificial intelligence (AI) and mixed, augmented and virtual reality (XR, AR and VR), along with the metaverse, digital twins and cloud computing, can transform the security and surveillance industry.



# Defining the stakeholder ecosystem

## Introducing SS-ECO

Traditionally, the OEM was at the centre of product design and development, but the situation has changed. The Security-Surveillance Ecosystem (SS-ECO) has matured, with multiple stakeholders now contributing to overall outcomes. A number of new stakeholders have entered the mix with the result that the SS-ECO is becoming better defined (Figure 1).

An SS-ECO comprises multiple participants ranging from manufacturers, distributors, system integrators, certification agencies, consultants and other entities, with each having roles and responsibilities designed to achieve key objectives and grow the industry.

While the ecosystem has end-to-end coverage, it is important to note that stakeholder concerns revolve around customers and their unique, specific and contextual requirements. These define personalised solutions for end users and drive adoption, optimisation and efficiency.

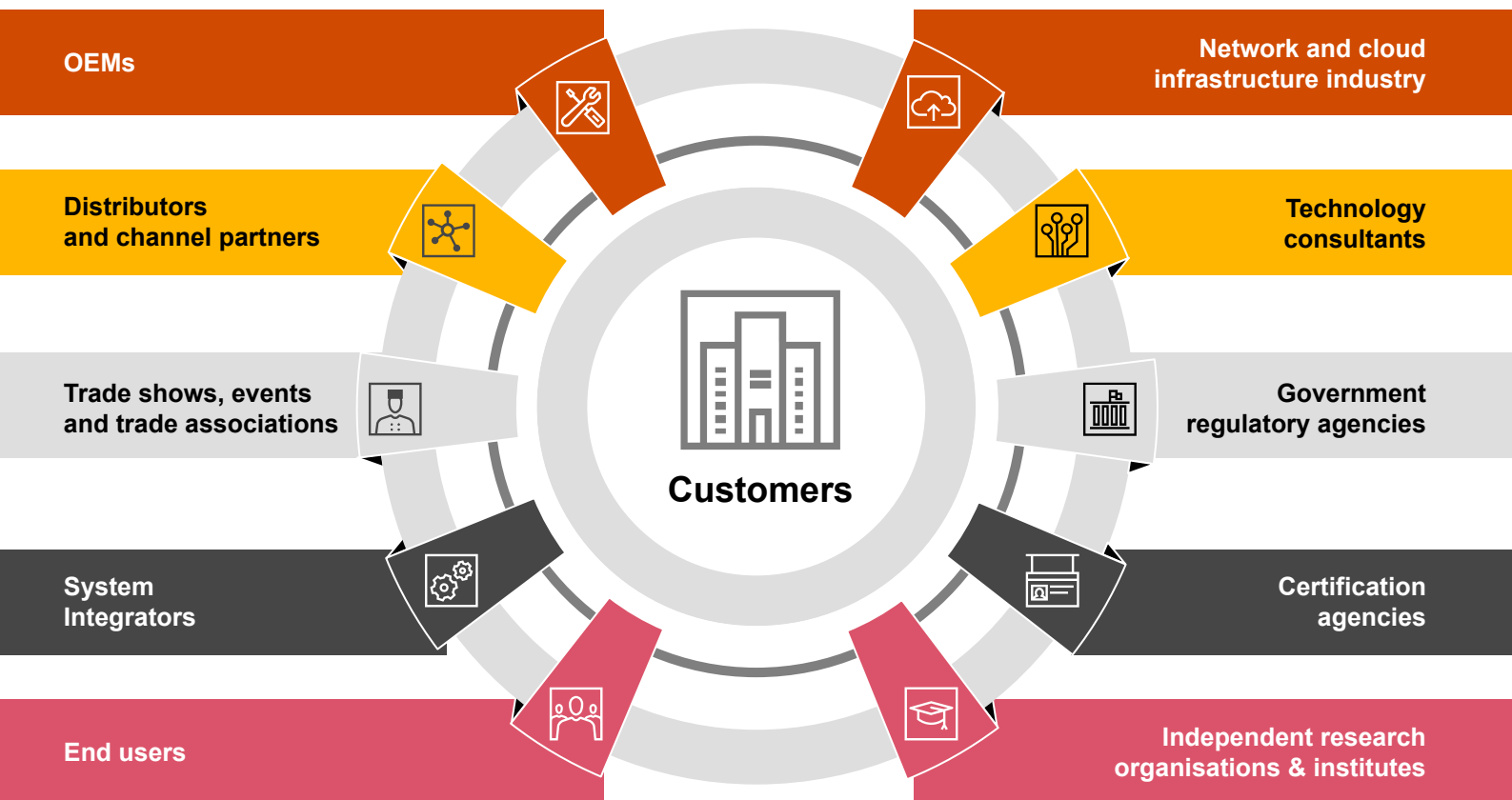
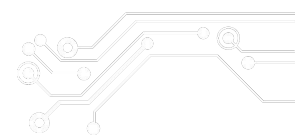


Figure 1: SS-ECO



## Let us take a look at the various stakeholders comprising the SS-ECO and how they play their respective parts



### Original equipment manufacturers (OEMs)

OEMs are manufacturers of security and surveillance hardware and software products, selling such products to channel partners and distributors. The primary OEM focus is on research and development to embed emerging technologies into their products, complying with changing regulatory guidelines and making vendor-agnostic products for easy integration into open architecture.



### Distributors and channel partners

Both OEMs and other technology firms are represented in specific regions by authorised channel partners. Business dynamics, the needs of the customer and compliance norms of the region are best known to channel partners. Channel partners also engage with distributors to deepen the supply chain and after-sales service.



### Trade shows, events and trade associations

These associations organise technology events and trade shows to bring together various solutions providers, end customers and industry experts on a single stage. Such events add real value to the ecosystem as solution providers get an opportunity to showcase their capabilities in the latest technologies and features, and end customers can see live demonstrations and gain a hands-on sense of the technologies they are interested in.



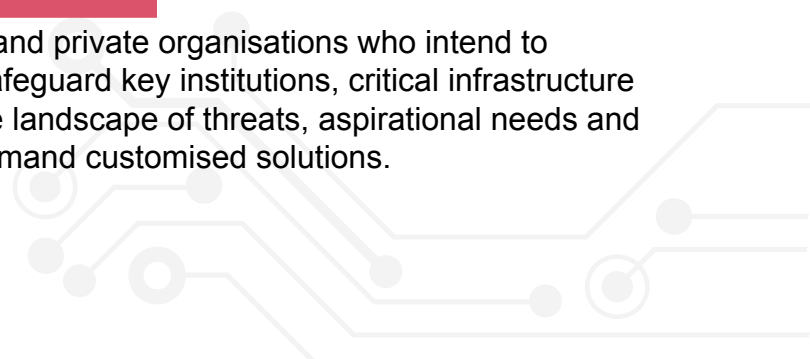
### System Integrators (SIs)

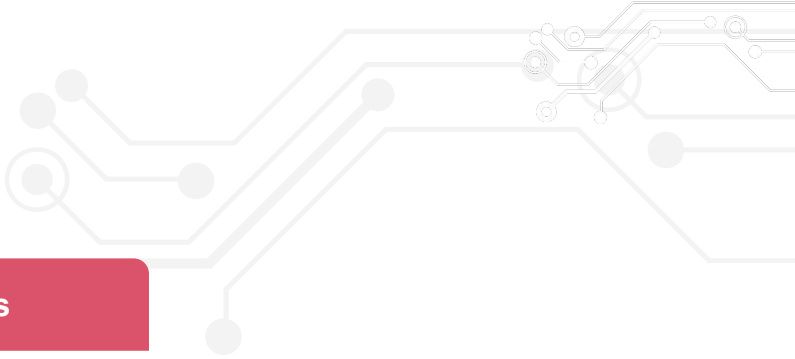
The SI is responsible for supply, installation, testing and commissioning of electronic security and surveillance hardware and software products for the project owner. The SI procures these products and is specialised in integrating various security and surveillance products according to project requirements. They are responsible for supporting operations and maintenance of the commissioned solution. A qualified and skilled SI workforce adds value to the whole ecosystem.



### End users

End users are government departments and private organisations who intend to implement security and surveillance to safeguard key institutions, critical infrastructure and citizens. Each end user has a unique landscape of threats, aspirational needs and customised requirements, all of which demand customised solutions.





### Network and cloud service providers

Network and cloud service providers manage and operate the network, compute, storage, and application/software services required for electronic security and surveillance projects. These services include internet access, last-mile network connectivity, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) cloud services. With the introduction of smart IoT (Internet of Things) devices and 5G networks, devices are able to directly communicate with the user with lower latency and high-speed bandwidth.



### Technology consultants

Consulting firms typically contribute an effective bridge between end users and technology solutions providers. They articulate customer requirements in technical/functional terms and communicate those to technology solutions providers. Their role is also crucial in helping end users to solve problems in the adoption of innovative technology, and the selection of viable technologies and reputable solutions providers. Project management consultancy services ensure the smooth implementation of complex projects.



### Government regulatory agencies

These agencies are responsible for providing frameworks and guidelines for developing and implementing security products and practices. The main objectives of these agencies are to safeguard national security by setting security guidelines for key institutions, critical infrastructure projects and to protect citizens. Typical regulatory initiatives include the General Data Protection Regulation (GDPR) in Europe, the Personal Information Protection Law (PIPL) in China and the draft Digital Personal Data Protection bill (DPDP) in India.



### Certification agencies

Given the critical nature of security systems, certifications are essential for organisations to gain the trust and attention of customers. Certification agencies are responsible for preparing standard norms and guidelines for the design, development, assessment and certification of security products and services. Certifications provided by these agencies ensure credibility and commitment in areas such as quality management, energy management, environmental protection and atmospheric safety.



### Independent research organisations & institutes

These organisations work independently to provide unbiased insights and statistics related to major technologies and trends in the electronic security and surveillance domain. Some organisations also set testing standards and evaluate products and solutions for regulatory compliance.

# Changing landscape

## Evolving customer needs

Customers in the security ecosystem aspire to provide a personalised experience to their end users. In seeking to deliver such experiences they have already gained a greater say in the overall product development lifecycle. However, in order to achieve strategic objectives, customers have been confronting challenges, including those of ecosystem interaction, product contextualisation and industry-led adoption.



### Scattered ecosystem players

Ecosystem players such as OEMs, channel partners, system integrators and other third-party entities collaborate to offer solutions with limited flexibility, causing unwanted lock-in.



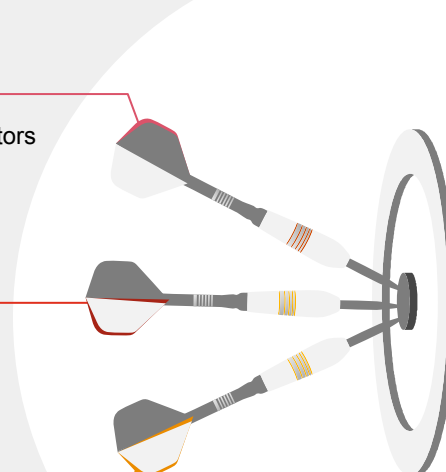
### Low solution contextuality

Global products are delivered with minimal use cases, lacking local relevance and contextual applicability for the solution.



### Industry-led reactive adoption

There is widespread acceptance of an industry-driven 'solution refresh' cycle without much consideration to innovation and disruption in the domain.



Lately, there has been a change in customer expectations aligned to the key challenges. These challenges have led to even higher expectations from the SS-ECO, whether they be in solutions, ecosystem development, customisation or innovation.



### One-stop access to resources

With innovative products and growing customer needs, customers prefer choice within integrated solutions and ecosystem services.

**For example:** the choice to procure cameras from a supplier, commission another supplier's video management solution and select another vendor's AI/analytics solution.



### Localised & contextual products

Customers have the responsibility to meet different localisation end-user requirements such as user experience, language and contextual use cases.

**For example:** co-creating use cases such as behavioural and gait analysis for providing access to people who have their faces covered.



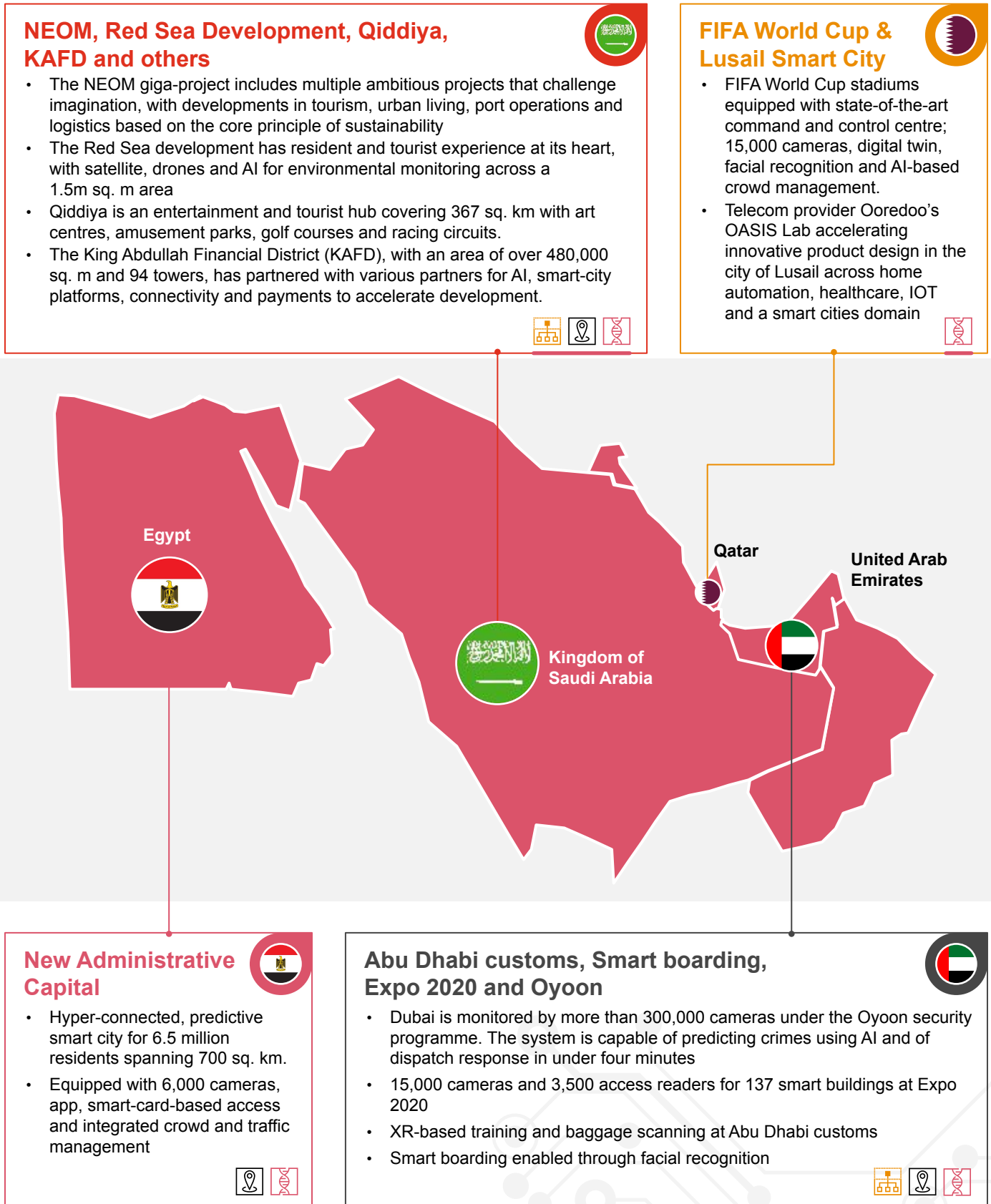
### Innovation in the DNA

Customers want to play an innovative role in the product development lifecycle, from concept design to prototyping, and become market disruptors and thought leaders.

**For example:** setting up innovation spaces, sandboxes, co-creation zones, new businesses and other dedicated facilities or departments to enable and sustain innovation.



In the Middle East region there have been unique and ambitious giga-projects (Figure 2) such as cognitive smart cities, mega-events and critical infrastructure with out-of-the-box visionary customer requirements for the security ecosystem. Such fast-evolving customer requirements have accelerated disruptive innovation in the industry. Where OEMs align capabilities with real-world regional requirements, this can enable regional as well as use-case specific products for the market.




















**Figure 2: Cognitive projects in Middle East region**

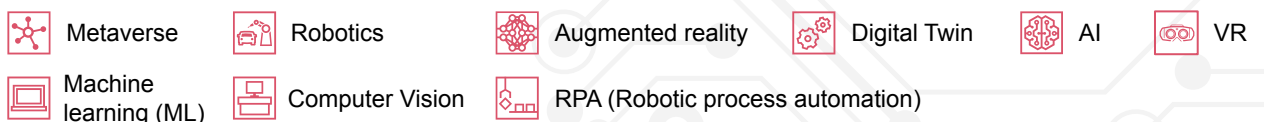
# Potential use cases



























Futuristic, yet real







Use cases that a few years ago were no more than moonshots for customers and OEMs are now feasible and viable thanks to rapid technological developments. Emerging technologies and their growing maturity have been key enablers to strategise, approach, plan and integrate security operations. With the advent of artificial intelligence, augmented reality, the metaverse, virtual reality, digital twins and cloud computing, the security industry is being transformed. These technologies are combining and feeding off each other in transformative ways to deliver impact that could help organisations to manage various kinds of threats for the foreseeable future.




## The top seven use cases that could transform the security and surveillance industry:

Use cases	Description	Emerging Tech	Outcomes	Country Adoption	Maturity Level
 <p><b>Digital twin simulations</b></p>	<ul style="list-style-type: none"> <li>• Creation of a digital twin using data from IoT sensors, geospatial and 3D visualisations</li> <li>• Use of VR headsets for an active experience of the situation from the remote location</li> <li>• Simulate different operational strategies and responses to deal with emergency situations</li> </ul>	 	<ul style="list-style-type: none"> <li>• Anticipate security issues</li> <li>• Highly accurate contingency plans</li> <li>• Enhanced performance</li> <li>• Optimise processes</li> </ul>	    	
 <p><b>Multisensory incident detection</b></p>	<ul style="list-style-type: none"> <li>• Audio analytics               <ul style="list-style-type: none"> <li>◦ Analyse and differentiate sounds (such as breaking glass, gunshots and emergency-response vehicle sirens)</li> <li>◦ Discern if people are conversing normally or if some have raised their voices and are engaged in an argument</li> <li>◦ Identify individual speakers based on their voice</li> </ul> </li> <li>• Smell analytics               <ul style="list-style-type: none"> <li>◦ Smell and detect a variety of complex smells</li> <li>◦ Detect gas leaks or the unusual accumulation of certain gases in a particular location</li> <li>◦ Locate hidden explosives, narcotics</li> </ul> </li> </ul>	 	<ul style="list-style-type: none"> <li>• Improved operational efficiency</li> <li>• Proactive incident detection</li> <li>• Invisible security control</li> </ul>	   	



Use cases	Description	Emerging Tech	Outcomes	Country Adoption	Maturity Level
 <p><b>Drone-based predictive crowd management</b></p>	<ul style="list-style-type: none"> <li>Correlating real-time and historical data captured from drones equipped with closed-circuit television (CCTV), thermal sensors, edge-based video analytics, and applying AI-ML to this data to predict where crowds are likely to gather</li> </ul>	  	<ul style="list-style-type: none"> <li>Informed intelligence</li> <li>Tailored contingency plan</li> <li>Situational awareness</li> </ul>	   	
 <p><b>Autonomous mobile units</b></p>	<ul style="list-style-type: none"> <li>Autonomous mobile units controllable via VR headsets equipped with IoT-based sensors (CCTV, thermal, LIDAR (laser imaging, detection, and ranging)) with ability to move in complex environments and communicate in real time using mission-critical communication</li> </ul>	 	<ul style="list-style-type: none"> <li>Enhanced on-ground coverage</li> <li>24/7 surveillance</li> </ul>	  	
 <p><b>Virtual command and training</b></p>	<ul style="list-style-type: none"> <li>Real-time VR-based virtual command-centre environment to remotely collaborate with multiple stakeholders for monitoring, controlling and managing incidents</li> <li>Realistic immersive training and gamification scenarios using bespoke simulations in AR and VR for public safety agencies</li> </ul>	  	<ul style="list-style-type: none"> <li>Removal of geographical barriers</li> <li>Enhanced situational awareness</li> <li>Increased user engagement</li> </ul>	 	
 <p><b>Bot-based command-centre operators</b></p>	<ul style="list-style-type: none"> <li>Deployment of self-learning AI bots as command-centre operators by emulating human intelligence to perform command and control centre (CCC) operations (sensor monitoring, anomaly detection, alarms processing, correlation and incident management)</li> </ul>	  	<ul style="list-style-type: none"> <li>Reduced manual intervention</li> <li>Prompt decision-making</li> <li>Reduced response time</li> </ul>	<i>Under R&amp;D Phase</i>	
 <p><b>AR-based screening</b></p>	<ul style="list-style-type: none"> <li>AR inspection to identify suspicious bags and manipulating such bags via gesture controls</li> <li>Information overlay on target individuals about their profile and threat levels from safe distance</li> </ul>		<ul style="list-style-type: none"> <li>Frees up space at chokepoints</li> <li>Real-time threat detection</li> </ul>	<i>Trialed by various customs entities</i>	

 Metaverse
  Robotics
  Augmented reality
  Digital Twin
  AI
  VR

 Machine learning (ML)
  Computer Vision
  RPA (Robotic process automation)

# Adapting to the cognitive wave

## Activating CSS-ECO

Evolving customer requirements demand localised products and innovative use cases. To achieve these objectives, a robust technology foundation is required to bridge the gap between expectations and reality. Emerging technologies are intertwined with core security systems, cognitive wrapper applications, visualisation layers and the SS-ECO. All these elements come together to form the Cognitive Security and Surveillance Ecosystem i.e. CSS-ECO (Figure 3).

The CSS-ECO differs from the traditional architecture in how it is designed and how information is exchanged between edge devices and end users. For years, edge devices/sensors have been sending raw data to on-premise applications for analysis and processing in order to manage complex day-to-day activities. This type of siloed architecture has limitations in terms of unlocking the potential for real-time detection, intelligent insights and proactive decision-making.

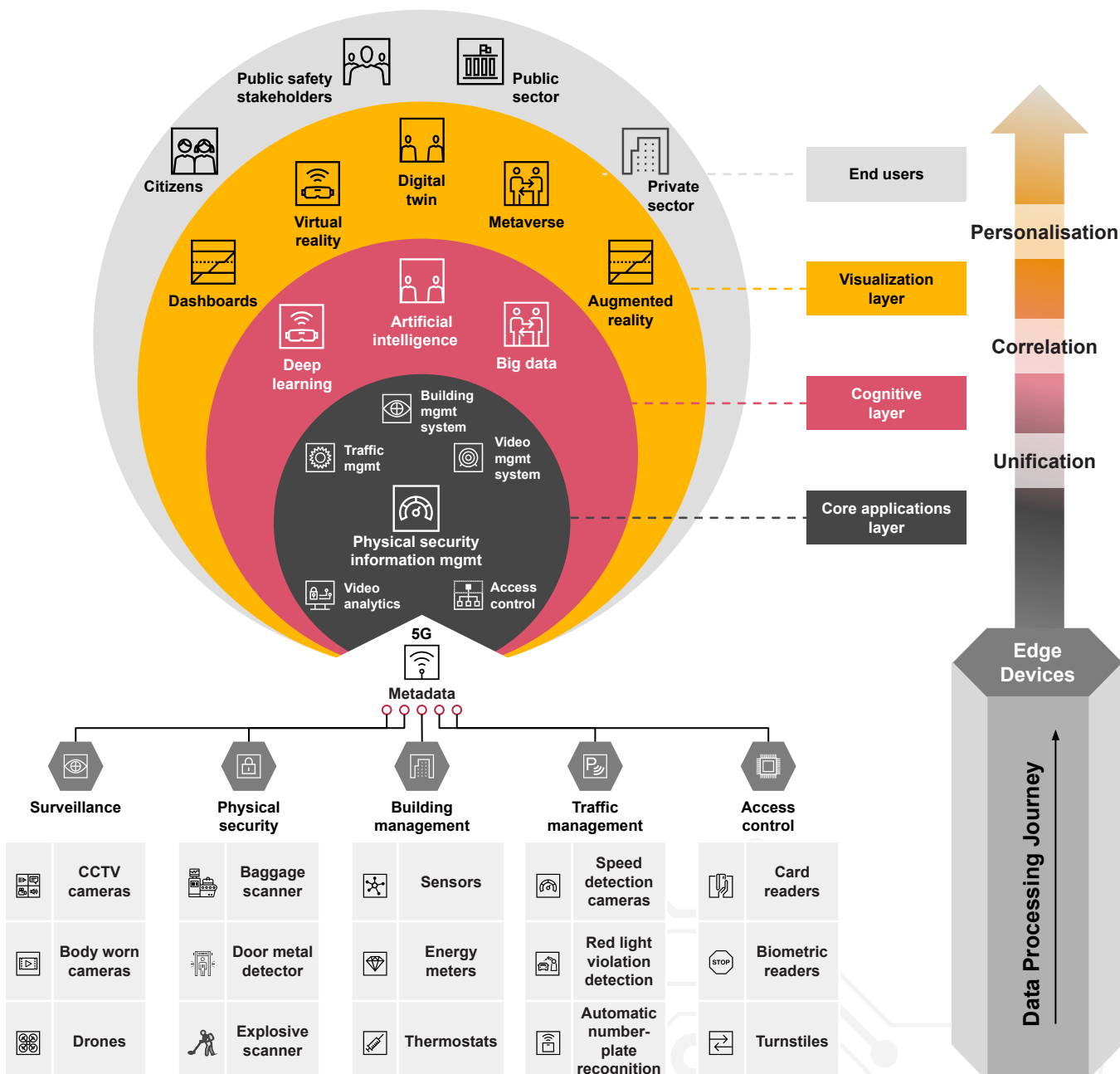
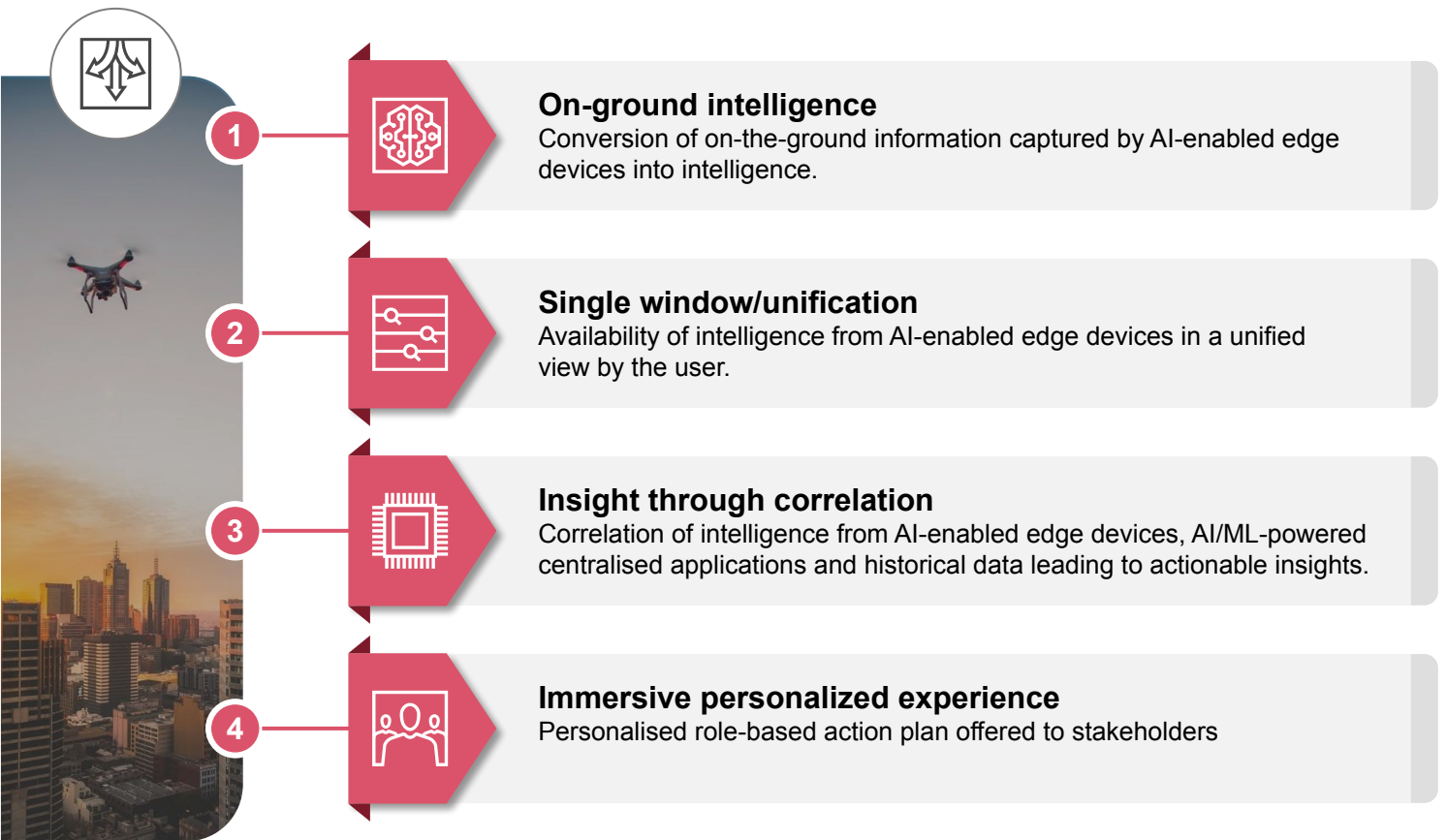


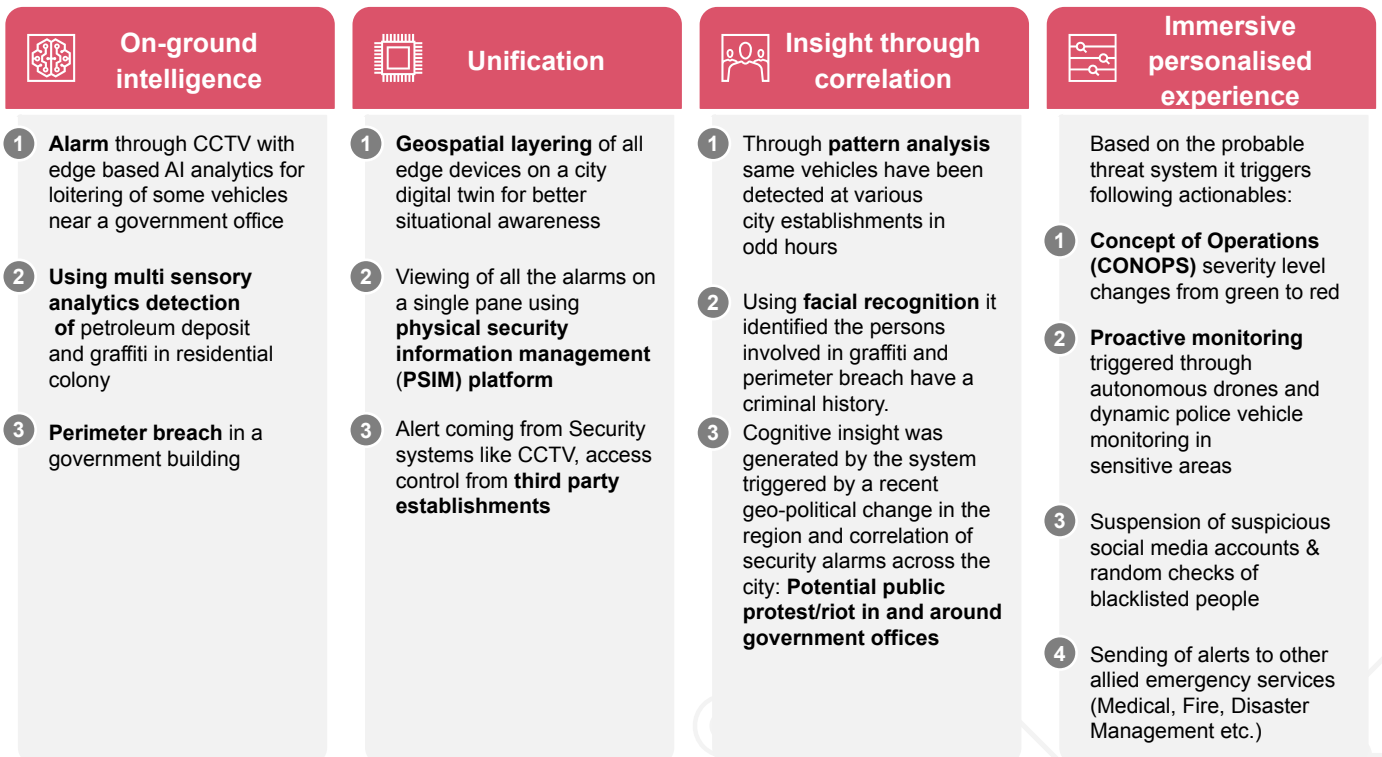
Figure 3: CSS ECO



# The flow of information in CSS-ECO



## Example: How the CSS-ECO gathers intelligence, preempts incidents and suggests proactive personalised actions to avoid crisis



# Customer-focused strategy

## Re-aligning the approach

To adapt the cognitive wave and tackle the changing landscape, OEMs and customers need to embark on a collaborative journey towards rapid innovation, enhanced quality and improved margins.

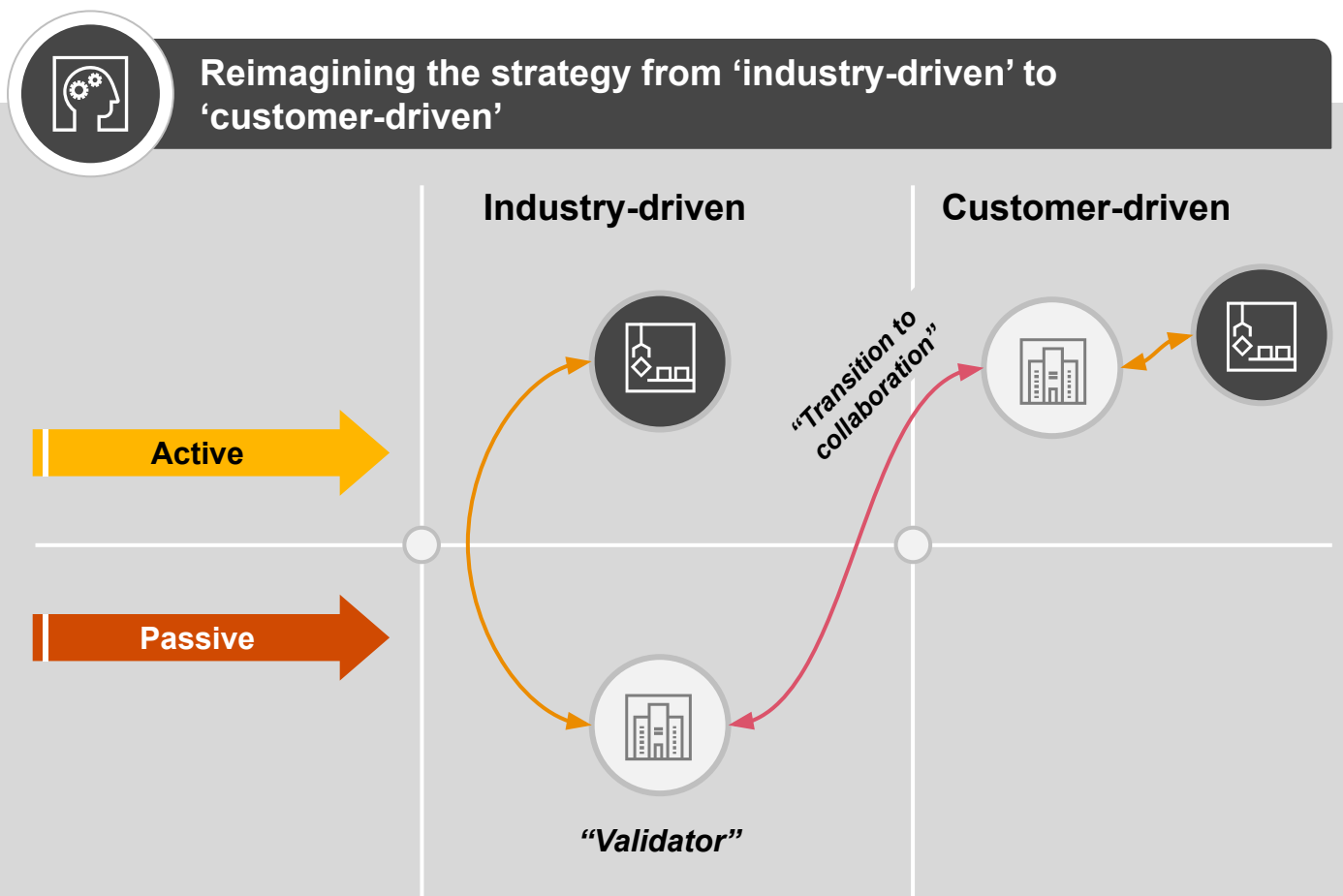
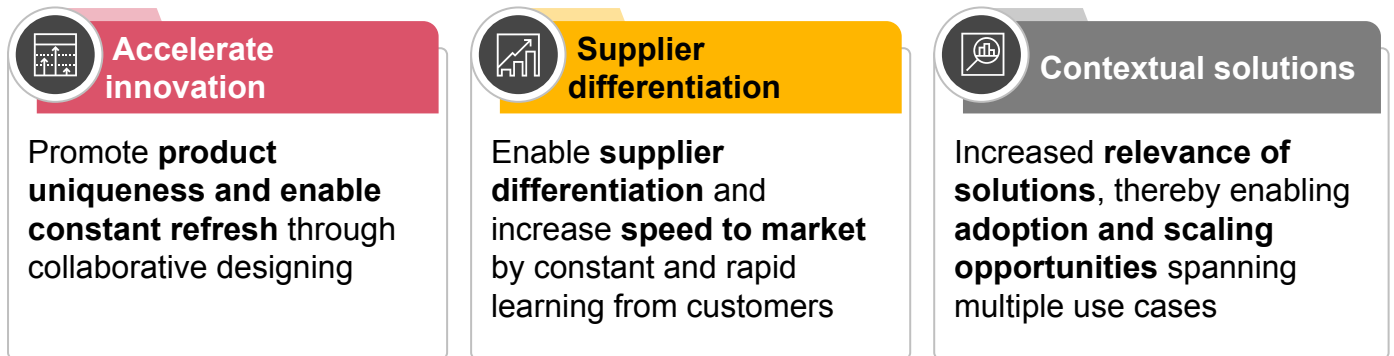
The challenges of constantly evolving customer expectations demand a transformation in the way customers and providers engage. Conventionally, OEMs have independently driven the industry across the overall value chain of the product, from concept, design and prototyping, to manufacturing and commissioning across various sectors and domains.

This process involved limited participation from customers. Product and service development was driven by in-house research and innovation at the OEM, while the customer only participated at the validation and adoption stage.

Today it has become imperative for the ecosystem to evolve and ensure active involvement from customers alongside their OEMs of choice. Proactive engagement should drive product development with customers' tailored requirements at the centre of the process. A shift towards a more collaborative co-creation model is required, with the customer and OEM engaging with each other and incorporating feedback throughout the product lifecycle.



A customer-focused strategy (Figure 4) should aim to accelerate the pace of innovation, as well as acceptance of the product, and drive OEM differentiation while keeping the end user at the centre of the overall value chain. It should ensure development of customer-centric contextualised solutions.

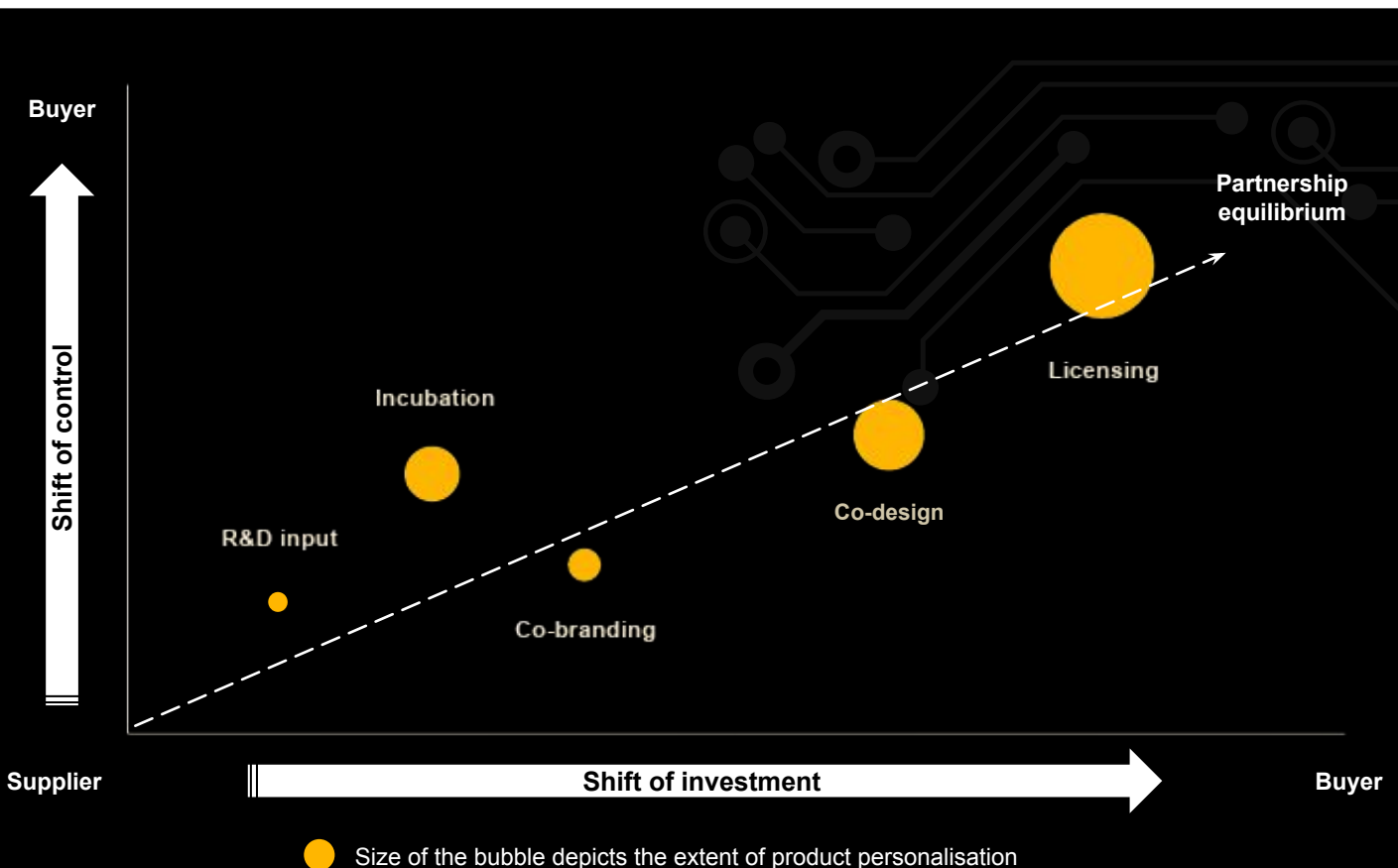
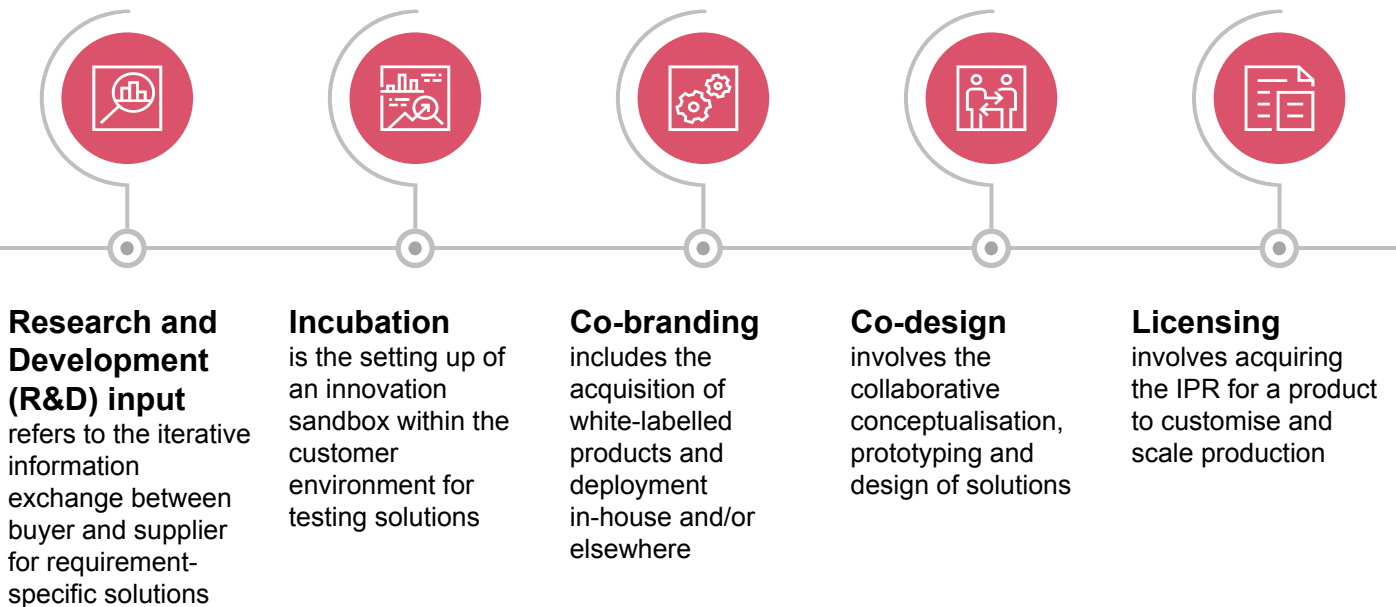


**Figure 4: Strategy shift to a customer-focused strategy**

# Levers of shift











## Accelerate innovation through partnerships

To play a more active role in the product design and development lifecycle, customers have a variety of levers they can use depending on their appetite for sharing of control and for investment, eventually leading to a personalised product (Figure 5).



**Figure 5: Partnership equilibrium**



Partnership strategy	Contribution to product development		Impact on product personalisation	Examples
	Control	Investment		
 <b>R&amp;D input</b>	Low	Low		ProdataKey has partnered with System Surveyor to provide its catalogue for import into the platform, making it easier for security professionals to build and cooperate on solutions using ProdataKey software.
 <b>Co-branding</b>	Low	Medium		The Viakoo IoT security platform has announced co-branding with PSA Security Network that allows PSA to benefit from Viakoo's products, preferential pricing and enhanced support.
 <b>Incubation</b>	Medium	Medium		Milestone Systems has dedicated business units for incubation. The mission is to create symbiotic partnerships that can help develop innovative ideas through open platform IP video development, driving new business and developing the marketplace.
 <b>Co-design</b>	Medium	High		Hailo has collaborated with Lanner Electronics in the creation of high-performance devices to analyse numerous video streams in real time on a single device, while securely delivering curated metadata and insights.
 <b>Licensing</b>	High	High		The acquisition of video security provider Qognify by digital sensor developer Hexagon expanded Hexagon's enterprise asset management capabilities with video monitoring provided by Qognify, introducing new markets and facilitating cross-selling.

It is important to note that a **partnership equilibrium** must exist in any partnership to succeed. The equilibrium will enable seamless design, development and scaling of a contextual and relevant product for the customer. There has to be a measure of equality in various decision factors such as vision alignment, information exchange channels and scope ownership. The partnership strategy is a function of a customer's position and approach on the available change levers and decision factors.

# Conclusion

Over the past decade there has been a rapid evolution in the security and surveillance industry. With emerging technologies playing a leading role in driving change across the ecosystem, the success and future of the security and surveillance industry lies in moving from an industry-driven strategy to a customer-focused strategy.

The shift can be enabled by partnership strategies with varying degrees of control and investment to strike a partnership equilibrium, while building a robust technology foundation as an enabler. This will require a collective effort throughout the whole ecosystem, working together to scan, assess and act on innovative customer requirements.

In this evolution, PwC will be there every step of the way to help enable the industry to create futuristic solutions to ensure a better, smarter, safer world.

And the journey continues.

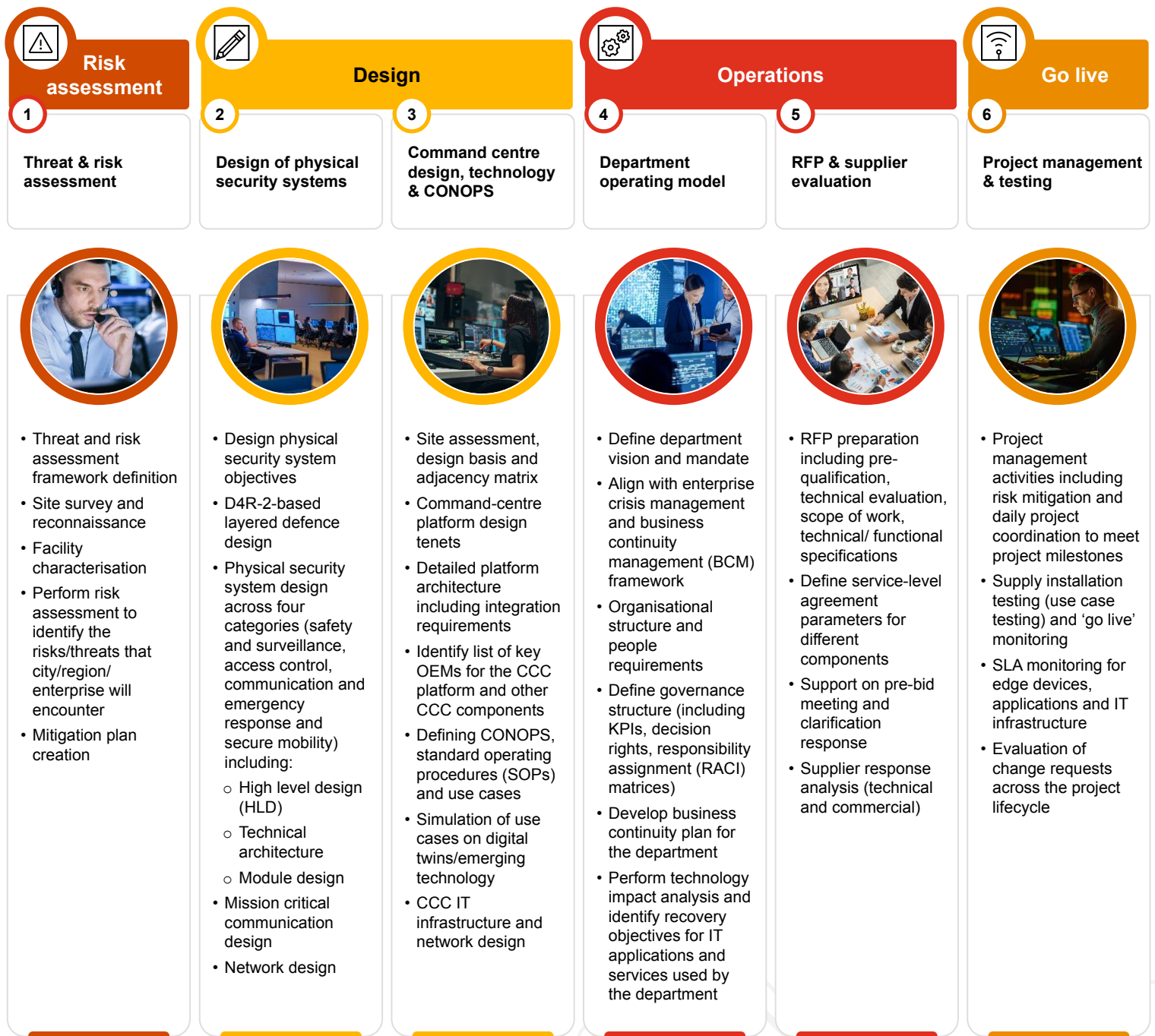
## References

1. <https://www.itpro.co.uk/strategy/29899/three-reasons-why-digital-transformation-is-essential-for-business-growth>
2. <https://tonomus.neom.com>
3. <https://www.neom.com/en-us/newsroom/neom-mclaren-racing-partnership>
4. <https://security.world/>



# How can PwC help you achieve your goals?

We are strongly committed to providing public and private-sector organisations with the tools required to develop or continue progressing their cognitive journey. We can deliver tailored services across the development stages of integrated physical security; from initial threat and risk assessment, to design of physical security systems, command centres and 'concept of operations' (CONOPS), to assisting in the development of operations in terms of operating models, RFPs and supplier evaluation, to the final step of ensuring a smooth launch of integrated physical security systems.



Integrated physical security development stages outline

# Contact us



## Rajat Chowdhary

Partner, Technology

PwC

Email: [rajat.c.chowdhary@pwc.com](mailto:rajat.c.chowdhary@pwc.com)



## Alpesh C Kankariya

Partner, Technology

PwC

[alpesh.c.kankariya@pwc.com](mailto:alpesh.c.kankariya@pwc.com)



## Sharang Gupta

Director, Technology

PwC

[sharang.g.gupta@pwc.com](mailto:sharang.g.gupta@pwc.com)



## Shailendra Singh

Director, Technology

PwC

[shailendra.singh@pwc.com](mailto:shailendra.singh@pwc.com)



## Vishesh Kalia

Senior Manager, Technology

PwC

[vishesh.k.kalia@pwc.com](mailto:vishesh.k.kalia@pwc.com)



## Himanshu Goyal

Senior Manager, Technology

PwC

[himanshu.c.goyal@pwc.com](mailto:himanshu.c.goyal@pwc.com)



## Dipesh Guwalani

Manager, Technology

PwC

[dipesh.g.guwalani@pwc.com](mailto:dipesh.g.guwalani@pwc.com)







At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 327,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at [www.pwc.com](http://www.pwc.com).

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries in the region with around 7,000 people. ([www.pwc.com/me](http://www.pwc.com/me)).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.