The digital transformation of security and the role of AI

How digital transformation and AI are reshaping security now and in the future.

2024

Contents

Introduction

Digital transformation is reshaping security. Increasingly driven by the exponential progression of Artificial Intelligence (AI) and cloud computing, this transformation is enabling and advancing security officers, processes and services in many new ways. It’s a changing world, and at Securitas we’re committed to helping our clients navigate and understand its potential for the security of their business.

Contributors

Morten Sommer Mikkelsen
Head of Solutions Offering
Securitas Europe

Olle Lindskog
Global Director
Securitas Operations Centers

Viking Johansson
Digital Director
Securitas Digital

Enhancing human roles with artificial intelligence

“The wealth of insight in security systems can support what is happening on-site in real time – for example, analyzing access control systems’ data to alert officers when more detailed evaluation of visitors is needed”

Viking Johansson
Digital Director
Securitas Digital

AI is already supporting businesses across diverse sectors and in security, this aspect of digital transformation is enabling automation of certain tasks, but what we are really seeing is the great potential of AI to complement and enhance the officer’s role, not supplant it.

“There will always be a place for security officers,” says Olle Lindskog, Global Director of Securitas Operations Centers (SOCs). “The human factor is irreplaceable in many environments, and officers fulfil a variety of roles. They are a reassuring and familiar front-of-house presence, they bring an informed understanding from their training and an intuitive awareness – from experience – of when something is not right. If action is required, for example evacuation of a space or interception of someone behaving suspiciously, they have the ability to make complex decisions and adapt to a rapidly changing situation. The value of AI is that it, in effect, gives them extra eyes and ears.”

Viking Johansson, Digital Director says, “The wealth of insight in security systems can support what is happening on-site in real time – for example, analyzing access control systems’ data to alert officers when more detailed evaluation of visitors is needed. It’s also used to give security managers the bigger picture and inform their decision making, for example for allocation of resources.” Digital transformation is also enabling the elimination of repetitive and monotonous aspects of the role – for example, AI’s abilities to rapidly filter and analyze live camera feeds and send real-time alerts mean officers are not just watching monitors waiting for something to happen.

“Leveraging these technologies makes good business sense, given the potential scarcity and cost of labor in advanced economies,” Johansson continues. “Upskilling and equipping security officers to connect and interact with these technologies adds interest and responsibility to their job, and this helps with recruitment and retention which, in turn, enables better service and security outcomes for organizations.”

The rise of remote

Digital transformation and emerging technologies have significantly fuelled the growth and capabilities of remote security services. As remote solutions have become smarter and more cost effective, individuals and organizations alike have embraced the ability to remotely monitor homes or premises via apps and browsers.

For some businesses, the COVID-19 pandemic accelerated the adoption of remote security solutions, as they prioritized measures to safeguard their people and sites. Remote monitoring and management capabilities quickly became an essential component for ensuring business continuity and resilience in the face of unprecedented challenges.

“A driving force behind the rise in remote security has also been the need for businesses to do more with less, and this is particularly true of regions where labor is comparatively more costly than security hardware and software” says Lindskog.

Cloud-based remote access control systems are a cost-effective way to significantly improve security. Authorized users can access the system anytime, anywhere, and monitor and maintain the security infrastructure across multiple sites, from a single device. Cloud solutions further enhance protection and resilience by enabling remote diagnostics, updating, and maintenance of security systems, eliminating the need to schedule physical site visits. And because cloud-based access controls are hosted on more than one remote server, business continuity is not disrupted if one goes offline.

Cloud-based video surveillance stores high-definition content (via IP cameras) along with encrypted, off-site back-up capabilities. So in the event that an on-site camera is damaged or taken out of commission, the cloud architecture securely stores all the video footage it has previously captured.

AI-enhanced remote surveillance is also contributing to more centralized, optimized operations, and enabling organizations to respond more swiftly to security threats – regardless of location. Skilled operators at security operations centers monitor video and remote access systems and verify and respond to alarms or potential breaches. These centers may receive millions of images and alerts each shift, so the use of AI and Machine Learning (ML) to identify patterns and detect anomalies and threats (in real-time) are revolutionizing the response process.

“Our use of AI analytics filters out up to 90% of false alarms. This consistency and accuracy means security teams can identify and focus their attention on genuine threats and react quickly, which improves security and service efficiency” comments Johansson.

AI POWERED CAMERAS – THINKING INSIDE THE BOX

AI enabled cameras and recorders incorporate advanced analytics functions that can detect and distinguish between people, animals, vehicles, and license plates. These capabilities are key to remote intrusion detection in and around buildings, even at long distances. The software can be programmed to work to multiple rules, such as only sending alerts if activity is detected at night, or not to respond if a movement is identified as being from an animal or a tree moving in the wind. If a genuine threat is detected, the AI-powered surveillance systems can send an alert to an on-site security officer, via mobile device, or to a SOC, detailing the location of an intruder or other security threat.

Capitalizing on the cloud

"Ultimately, we see cloud migration as being a vital foundation for the expansion and agility of security services"

Morten Sommer Mikkelsen,
Head of Solution Offerings
Securitas Europe

"Many businesses have spent the last few years migrating central components of their business operations to the cloud," says Morten Sommer Mikkelsen, Head of Solution Offerings, Securitas Europe. "The next natural development is to move their security systems' servers off-premises as part of a 'cloud-first' strategy. And since AI's enhanced detection and data analysis capabilities demand huge computing power, this is likely to accelerate the move."

The hardware-free and serverless architecture of the cloud offers many benefits for a security infrastructure. It's more reliable and efficient, and easy to use and manage. Businesses do not incur the expense of rack storage, power or hardware on their site, nor the need for specific software. The computing capacity can be rapidly scaled up or down, and since cost is directly linked to usage, the organization only pays for the computing power it needs – reducing operational costs.

For some organizations however, concerns about cybersecurity still create a barrier to adoption of cloud-based solutions.

"It's an understandable concern but moving to the cloud can increase cybersecurity, and risk can be mitigated by putting robust systems and processes in place," continues Sommer Mikkelsen. "A starting point is to create strong separation between what is company related and what is security related, for instance, incorporating an endpoint protection system defending all servers and devices (e.g., desktops, laptops, mobiles) from malicious activity. Ultimately, we see cloud migration as being a vital foundation for the expansion and agility of security services."

Leveraging security systems for business insight

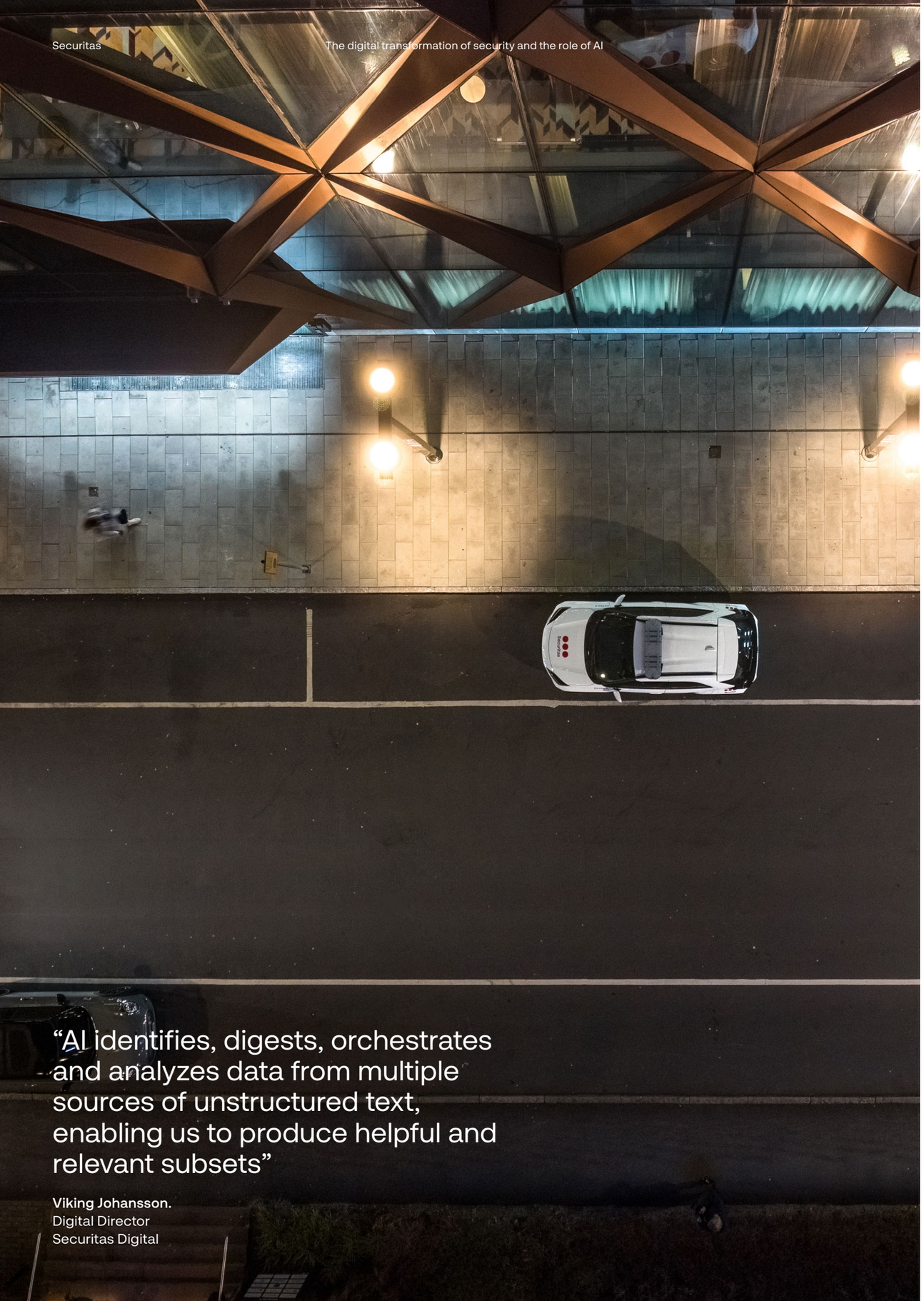
Although digital transformation in the business world is not new, it is only relatively recently that the value of ‘big data’ has really begun to be leveraged. In the security sector vast quantities of data are generated by multiple sources, for example via regular reporting across hundreds of sites, events and individuals, and millions of security sensors and devices.

“AI identifies, digests, orchestrates and analyzes data from multiple sources of unstructured text, enabling us to produce helpful and relevant subsets,” explains Johansson. “From this qualitative analysis we can identify patterns, and better predict what will happen. This insight can then be used by the business for strategic decision-making, for example to streamline and rationalize allocation of security budget and resources.”

With security increasingly on the boardroom agenda, this is a timely development. Now, stakeholders can gain real insight on everything from the current threat landscape for their business operations in different regions, to matters of regulatory compliance. They can use this insight to actively mitigate risk and identify opportunities for operational improvement at every level – from deciding where to allocate resource across whole regions, to optimizing a single security officer’s route around a site. AI-analysis of data can also be used for real-time ‘health reporting’ across electronic security systems, monitoring performance and status. And if an issue arises technicians can quickly be alerted, thus increasing resilience, and reducing risk.

In addition to supporting organizations’ security risk management, the wealth of actionable insight stored in security systems can contribute to wider business intelligence and supporting decision-making in other operational areas such as marketing, sales, and HR for instance, visitor heat-mapping or footfall.

Soon, the natural progression of these intelligence-led capabilities will see increasing integration of security systems with other building management systems in pursuit of cost efficiencies and sustainability. For example, security sensors that are in place to detect intruders can also be used to detect and switch off unnecessary light and heat/cooling in unoccupied spaces.



“AI identifies, digests, orchestrates and analyzes data from multiple sources of unstructured text, enabling us to produce helpful and relevant subsets”

Viking Johansson.
Digital Director
Securitas Digital

Security as a Service - a foundation for security solutions

Just as Software as a Service helped drive digital transformation, and vice versa, the digital transformation of security is fuelling the rise of ‘Security as a Service’ (SECaaS) which offers organizations the benefits of end-to-end security solutions with built-in scalability, accessibility, efficiency, and economy.

“When we talk about end-to-end security solutions, we mean the provision of everything, within an agile and dynamic framework” explains Sommer Mikkelsen. “From risk awareness and assessment, through solution design and implementation. This may include hardware, software, security officers, systems and ongoing monitoring, maintenance, and advisory services.”

But it’s not just about services, costs and efficiencies. It’s about trust and relationships. Security is a multi-layered proposition and as technology-driven solutions proliferate, more organizations are looking to work with a single provider. They want a partner that can understand, and anticipate their needs, and help them leverage the super-powered security solutions of the future.

“Organizations are not looking for a merely transactional relationship, they want a trusted partner” says Lindskog. SECaaS looks set to become an integral element of that partnership.

Conclusion

From on-site officers to invisible cloud-powered solutions, security will continue to traverse both the physical and digital space. And while the digital transformation of security is well underway, the full potential of unique human capabilities combined with the power of technology is yet to be fully exploited, or even imagined.

What is not in doubt is that, for the foreseeable future, the best security will demand the best of people and technology, and the essential link between them – connectivity. With a global presence and expertise, Securitas is at the forefront of the digital transformation of security and will remain so.

At Securitas we are taking the security industry into the future. We bring together our expertise in individual services such as Remote, Mobile and On-Site services, Fire & Safety and Technology, into innovative security solutions to meet our clients' diverse needs. Just like your business, our security solutions are built to adapt and grow. And with a truly global presence, we are proud to be trusted security partners to businesses all over the world.