

# Optimize Security and Transform Operations

Building a Case for  
Virtual Guard Solutions

The Intel logo is displayed in white text on a dark blue background. It is positioned in the upper right quadrant of the image, partially overlapping a large, stylized padlock graphic. The padlock is rendered in a light blue, isometric style with a dark blue keyhole. The background of the entire image features a complex network of glowing blue lines and nodes, suggesting a digital or cyber environment.The Convergent logo is located in the bottom left corner. It consists of the word "convergent" in a lowercase, sans-serif font, with a red vertical bar separating the "conver" and "gent" parts. The logo is set against a dark blue background with a network of glowing lines and nodes.

# Team

## AUTHORS

**Robert van den Heuvel**

Business Intelligence Manager, Convergent

**Kasia Hanson**

Global Sales Director, Safety & Security and Safe Cities, Intel®

## EXECUTIVE SPONSORS

**Eric Yunag**

VP of Technology & Innovation, Convergent

**Amir Shechter**

Executive Director of Digital Transformation, Convergent

**Jen Bossin**

Senior Director, IoT Partner Scale, Intel

## CONTRIBUTORS

**Erin Planting**

Digital Marketing Manager, Convergent

**Jen Bossin**

Sales Director, IoT Partners, Intel

**Connor Quigley**

US IoT Partner Marketing Manager, Intel

**Mary Parisi**

Marketing Specialist, Convergent

**Rob Risany**

Director, Edge AI Solutions Architecture, Intel

**Mike Trojecki**

Director, Edge AI Solutions Architecture, Intel

**Will Stewart**

Edge Partner Sales: Digital Safety & Security, Intel

*“The contemporary landscape demands that businesses of all types implement a robust and forward-thinking security posture. This involves alignment on strategies, methodical program implementation, and comprehensive solutions focused on driving operational efficiencies throughout the organization. At Convergent, we believe in a layered design to ensure maximum performance and functionality, reducing costs and risks by deploying the best of what’s available via digital technology to complement physical security assets.”*

**Eric Yunag**

**VP OF TECHNOLOGY & INNOVATION,  
CONVERGINT**

*“In the world of organizational security, advanced technology provides the required backbone that powers a broad array of leading-edge solutions. Intel technology, from our CPUs to software development tools, support the highest levels of performance, enabling our partners' clients to take advantage of enhanced media and AI capabilities, IoT-related features, and more, all while using less power and leveraging the best of what’s available today.”*

**Jen Bossin**

**SENIOR DIRECTOR,  
IOT PARTNER SCALE, INTEL**

# Overview

In nearly every industry, pressing challenges ranging from labor shortages to rising operating costs and more continue to drive change in the way businesses manage employees and production. The increased urgency for digital transformation taking place all around the globe has further impacted the ways in which organizations manage the security and safety of their various physical environments. From airports to healthcare facilities, corporate headquarters to monitored parking structures, the need to maintain a high level of security and safety for employees, visitors, real estate, and data has never been greater. This need is met with ever-increasing challenges related to the hiring, training, and retaining physical security guard personnel. Given today's competitive job landscape, where minimum wages are increasing and multinational technology and e-commerce companies continue to extend their footprint into more cities and offer high-paying employment opportunities, turnover and burnout for security staff has never been greater. And these realities will likely increase in the years ahead.

When it comes to navigating these challenges, however, there are options available to nearly all organizations. By coupling the best of what's available via technology with the strategic use of highly valuable physical security guards, businesses can implement a comprehensive augmented guard

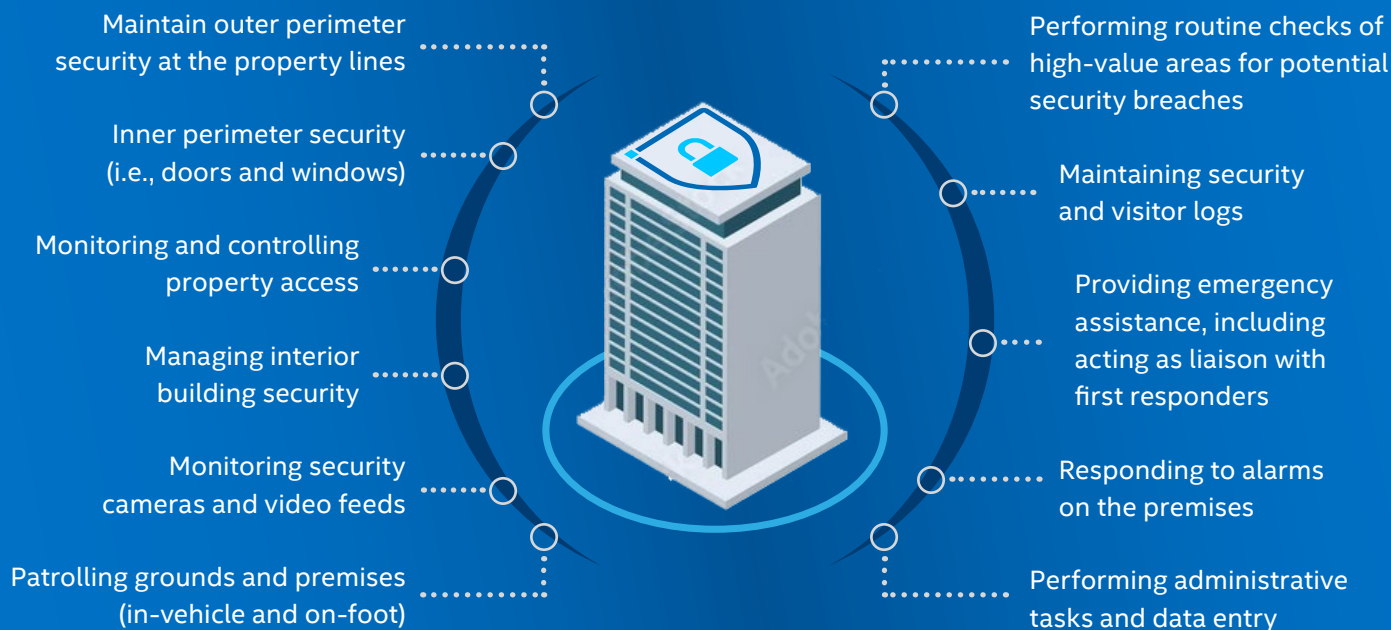
experience and improve their overall security posture while reducing costs, mitigating risks, and optimizing operational processes.

## Current Market Trends

In order to perform the task of maintaining building security, organizations have most often chosen to employ or contract out physical security guards, whose responsibilities include maintaining law and order, reacting and responding to emergencies or threats, greeting and assisting visitors, patrolling a building's grounds, and providing access control. For many companies, the mere presence of armed security guards is enough to ensure a level of safety for employees, visitors, and the building itself. In some instances, guards may also perform administrative duties like keeping a visitor log or assisting with directions around a physical campus, maintaining a high level of vigilance for things like chemical leaks or other potential risks, and informing responders about the details of an emergency when law enforcement, fire department personnel, or EMTs arrive on the scene.

Building security encompasses all the ways in which an operations manager or team safeguards people, assets, and physical property, ensuring that data and sensitive corporate information remains safe and secure. The goal of a well-conceived

## Physical Guard Duties





building security strategy is ultimately focused on the prevention and detection of incidents (as well as the response to them), ranging from theft and vandalism to general access control for visitors. While it may not be reasonable or even possible to prevent every incident from occurring, decreasing the likelihood of incidents can be achievable, especially when a comprehensive security posture has been implemented and maintained over time, evolving as threat landscapes change.

As technology has evolved and more companies are implementing advanced security systems built on complex platforms and capable of providing greater analysis, the demands on security guards and their job requirements have increased proportionally. The world of cybersecurity has become more and more sophisticated in recent years, flooding the market with an abundance of new technology. AI, ML, IoT and other technologies offer numerous tools and techniques that, when coupled with existing physical security systems and personnel, converge to create new methods for ensuring building security and the safety of employees and visitors within corporate environments.

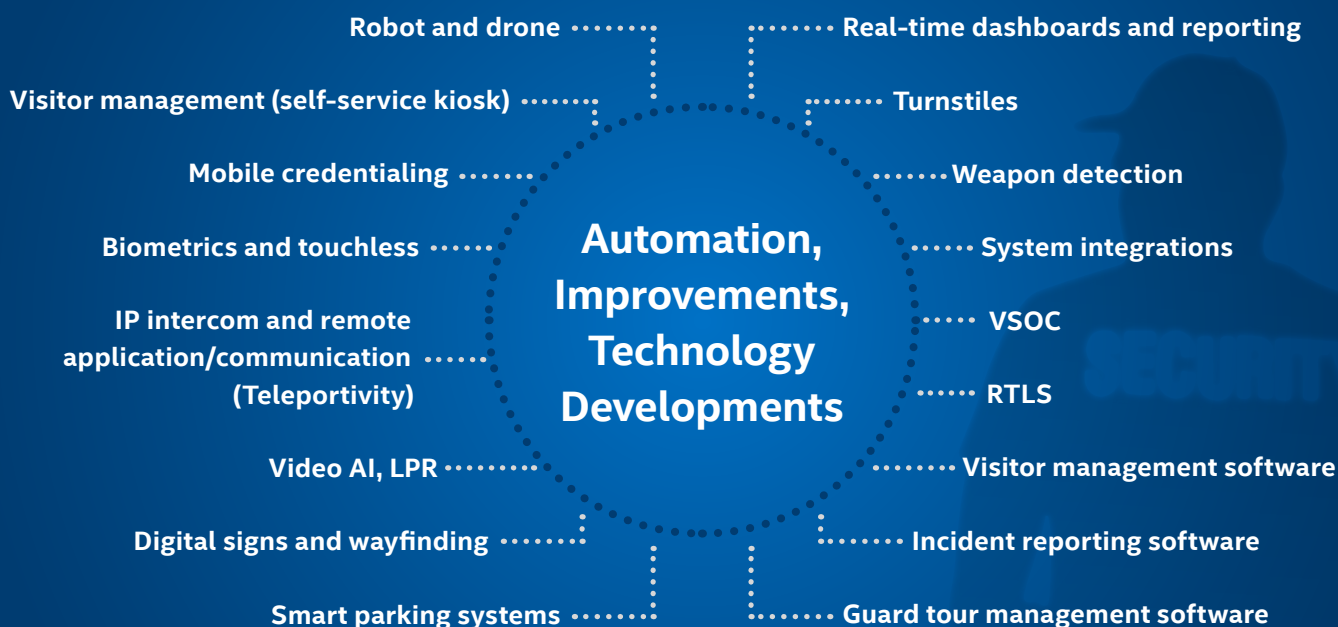
In the wake of a global pandemic that forced much of the workforce to find alternatives to on-site employment, workers are returning to work in increasing numbers. Many of these employees have uncovered new and dynamic ways to fulfill the duties of their jobs, including virtual and part-time or work-from-home solutions.

## 1 Dispelling 3 Common Myths About Digital Security

**Myth 1:** Technology cannot fully replace the effectiveness of a physical security guard.



**Reality:** For most organizations, physical guard services won't be universally replaceable. However, a 20–30% reduction in guard services is a reasonable benchmark for many companies. In reality, some repeatable “non-complex” tasks can be easily replaced by technology, enhancing the customer experience while reducing friction. Optimizing technology, people, and processes can generate significant savings for large companies already spending tens of millions of dollars on guard services. Self-service visitor kiosks, virtual intercoms, AI/ML video applications, biometric verifications, tailgating technologies, drones, and robots are all examples of technologies that can augment human abilities and optimize security while improving performance and efficiencies.



Similarly, organizations equally impacted by fulfill the duties of their jobs, including virtual and part-time or work-from-home solutions. Similarly, organizations equally impacted by Covid underwent rapid digital transformation, implementing new and innovative solutions that were essential to maintaining operations with so many workers no longer physically available. In many instances, companies experienced shrinking footprints together with the need to secure facilities with fewer people than before. Here, comprehensive and scalable security solutions for building security have become routine for organizations across many industries.

As people return to physical buildings for work or recreation, the future of security and safety is advancing through the use of these technological solutions, which can assist stakeholders and customers to achieve their security and operational efficiency objectives.


As a result of these and other realities, many of the challenges associated with adopting new, cost-prohibitive technologies have been solved. Today, easily implemented and readily available digital solutions can be used to re-engineer traditional security processes in a manner that makes financial sense.

## Organizational Security Challenges and Risks

In terms of the employment landscape, organizations face several co-existing challenges when it comes to hiring, training, and retaining security personnel. Total employment of security guards and safety officers across the broader economy is projected to grow as much as 15 percent from 2020 to 2030, a figure that represents faster growth than the average for all occupations.<sup>1</sup> Government agencies are advising that as many as 165,000 jobs on average for security guards are projected to open every year for the next decade.<sup>2</sup>

While the job market has demonstrated a 21% wage increase over the last five years for security guards, workers in the industry are still paid more than 25% below the national average. With the rapid rise in technology, novel solutions to existing security concerns are becoming more readily available, further challenging the role and value of physical security guards. One example—the security robot market—had an estimated value in 2018 of \$2.1 billion, and is currently on pace to grow at a CAGR of 7.93 percent to reach \$3.3 billion by 2024.<sup>3</sup>

### Challenges within the security guard industry:

- 
- Employee and training and turnover costs
  - Employee availability
  - On-the-job risk and safety issues
  - Employee turnover and process optimization
  - Employee job satisfaction
  - Regulatory and compliance issues
  - Repetitive tasks and fatigue
  - Physical interventions
  - Response time
  - Nighttime and after-hours security issues
  - Complexity of tasks and task management
  - Element of human decision making in security and high-risk emergency situations
  - Armed guard training and management
  - Human interaction
  - Reduction in efficiency and customer satisfaction or experience within buildings

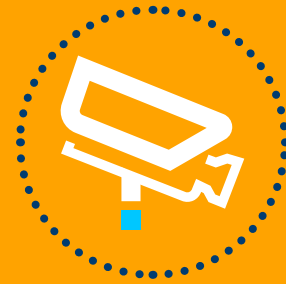
For security guard firms, people—not technology—remains the most significant cost, with the numbers running upwards of 95%, resulting in extremely tight margins for profit, which are often dependent on just a few percentage points. Here, one of the biggest challenges that can impact these fragile margins is one that guard firms may not immediately have visibility into—unbilled overtime. This oversight can create as much as a 6-10% impact reduction in profits. For the owners of security firms, the importance of identifying and controlling costs while finding ways to prevent non-billable overtime remains a high priority, and a challenge that too often goes unnoticed.

Although there will likely always be a need for physical security guards to maintain the safety of personnel and buildings, especially when certain processes require human verification, the application of technology and digital solutions often makes more sense. For example, where concealed spaces may present a challenge for security guards who would need to dedicate valuable time to physical patrols, cameras and live video feeds can provide important services like temperature detection, while IoT devices are available for moisture or chemical detection. Similarly, when considering large building campuses that require multiple physical security guards in order to maintain comprehensive security, drones can effortlessly cover large areas. When building occupancy scales down (i.e., during a night shift when an organization is closed to employees and visitors), digital video monitoring can alleviate the need for multiple security guards. They no longer need to physically patrol building spaces, and can instead simply monitor video feeds for suspicious activity.

Many of the challenges involved with the use of physical security guards come down to cost and availability, two factors that continue to present outsized obstacles for security firms and organizations alike. Given minimum wage rising in many areas as high as \$15, with an additional \$5-6 tacked on for benefits (healthcare, vacation, pension/retirement, etc.), security personnel represents a significant budgetary expense. Based

## 2 Dispelling 3 Common Myths About Digital Security

**Myth 2:** Autonomous entities like drones and robots will take over all patrolling duties.



**Reality:** The increased capabilities of autonomous drones and robotics means that they can now be integrated into a multi-sensor security protection system, offering the ability to automatically respond to alarms and events triggered by the detection system. In addition, the system can initiate autonomous scheduled tasks for security and non-security purposes. Through the use of autonomous tools, security personnel can increase safety and security operations while optimizing detection, response time, and risk reduction.

on 2000 annual working hours at the adjusted rate of \$23-25 per hour for security guards, the cost for one security professional can run as high as \$50,000 a year. In some areas, as much as 15% of security guards may only work part time, which places an even greater burden on firms to train and retain qualified employees.<sup>4</sup>

Many organizations consider security costs and guard services to be overhead, with little ROI available for the expense, leading to reduced job satisfaction for security personnel. The rise of major employers in the tech sector (i.e., Amazon and Google) has flooded the job market with high-paying employment opportunities that don't require specialized skills or advanced education—providing a clear example of where members of the labor force are moving to, while exiting jobs in areas like physical security. Further complicating the employment picture, annual turnover rates for security guards is estimated to range from 100% to 300%, meaning that most security personnel exit the job in the first year, with many guards leaving their post in the first four months.<sup>5</sup>

# Benefits

As a result of these ongoing challenges, organizations everywhere are upgrading their operations and physical building security to incorporate connected and intelligent technologies. Comprehensive digital technology solutions powered by high-capacity computing can help stakeholders realize several benefits to security and operations by adopting smart features and connectivity. Given the challenges that organizations face when it comes to security, many enterprises are asking themselves—What if there's a new way to accomplish our security and safety objectives? What if technology offers solutions that can augment our existing security strategy, alleviating the need for some guards while delivering a more robust security posture?

## Optimizing Processes and Enabling New Use Cases

Organizations can implement a range of digital security solutions that transform and improve operations, provide key insights, and enable new use cases. Leveraging the best of what's available in terms of rapidly evolving technology, nearly every industry stands to benefit from the adoption of virtual security solutions.

## Lowering Costs, Improving Customer Service, and Increasing Safety

Organizations across a multitude of industries stand to increase the value of their security processes

through the efficient implementation of digital solutions. In the process, these organizations can leverage the power of technology to deliver greater insights, enhanced security, and cost-effective ways to modernize existing legacy systems or to improve outmoded, labor-intensive, and inefficient ways of securing buildings and on-site personnel.

Several security instances can be implemented in an effort toward process optimization that involves replacing or reducing the use of physical security guards, and augmenting those duties through technology. This may include things like replacing security guards stationed in a building lobby with digital kiosks, substituting physical security details in remote building or campus areas with video security technology, or reducing risk to physical security personnel through drone technology on nighttime patrols or in high-risk and remote areas. Similarly, through the implementation of digital security technology solutions, organizations can improve hiring and training practices, reducing the costs and overhead associated with employee retention issues and hiring fewer physical security guards—one among many of the benefits available via smart security elements.

When considering an example like digital kiosk use in a building lobby area, organizations can also offer an enhanced customer experience for visitors, many of whom already understand how to get what they need without human interaction, and may prefer it. Organizations can retain physical security guards solely to perform complex tasks



## Industries that can make use of virtual security measures:



Healthcare



Transportation



Energy



Financial



Retail



Public venues



Manufacturing



Real estate and offices



Datacenters



requiring human interaction such as welcoming visitors, answering complex questions, aiding with slip-and-fall incidents, or performing physical sign-ins. Technological solutions are also available to expedite building and parking lot entry for visitors, thus eliminating redundant or unnecessary costs for things like information desks and physical security guards through automation, smart security features, digital signage and kiosks, parking lot monitoring, vehicle entry gate technology, mobile credentialing, managed service, and more.

With technology rapidly evolving and greater acceptance of digital solutions becoming the reality of the day, companies are spending more and more on training and education, devoting significant resources and money to things like physical security guards. As enterprises continue to demand customized security solutions based on their unique needs, digital technology can be used to create security guard solutions that blend seamlessly into a specific corporate culture, streamlining training processes and operations. These solutions have the capacity to improve recruiting, onboarding, and retention of staff while paying mind to increasing wage gaps that may lead to difficulties in market competitiveness. Through the reduction of high staff turnover, including the time and expense of training and onboarding new security guards, organizations can create greater efficiencies in the use of internal resources.

### 3 Dispelling 3 Common Myths About Digital Security

**Myth 3:** Deployment cost for digital security is just too high and is not a solid ROI.



**Reality:** As the threat landscape grows alongside the rapid adoption of IoT devices and remote workforces, the reality of a security breach becomes increasingly imminent for organizations both large and small. Given the outsized costs associated with hiring, training, and maintaining a physical security guard force, together with human limitations in many common scenarios, investing in a proactive and holistic digital security infrastructure and deploying applicable technologies represents a solid return on investment for organizations in nearly all cases.

### Enhancing Physical Security and Reducing Risk

With digital technologies, organizations can enhance physical security throughout any building environment as customers return to public





spaces and employees head back to the office. By intelligently leveraging digital security solutions powered by advanced technology, companies from all industries can create safer and more secure environments for customers and employees.

As security guard tasks grow in number and complexity through greater adoption of technology—including things like facial authentication, AI, ML, and data analytics—the role of the security guard has become more challenging and difficult for organizations to fill. Digital solutions are available to relieve some of that complexity, and in many cases, physical security instances can be replaced or improved by technology. This includes things like compliance and regulatory updates and issues, using digital solutions to efficiently manage an ever-changing landscape with automation; improved access control, allowing only authorized visitors into an area while keeping uninvited

people out; increased building perimeter and parking lot security, and more.

By saving costs and resources typically spent on physical guards through available digital technologies, companies can invest the “savings” on only the required number of highly skilled, well-trained guards. By paying them a competitive wage, firms and organizations will dramatically improve employee retention, drawing security personnel deeper into company culture and making greater investments in job satisfaction. Given all the market challenges and potential benefits associated with the adoption of virtual security solutions, implementing a new model of comprehensive security is more crucial than ever. With the technology available today, organizations would be well served to take action now, rather than standing by and waiting to see what the security market will look like in five or ten years.

## Enhance Physical Security and Reduce Risk



# Convergent and Intel Platforms

Organizations of all sizes from a broad array of industries can take advantage of high-performance computing platforms for the processing power to capture, monitor, and use data from technology-equipped security appliances for greater insight into operations and improved environmental safety and security.

The latest Intel technologies built into 12th Gen Intel® Core™ processors along with software development tools such as Intel® Distribution of OpenVINO™ toolkit and Intel® oneAPI IoT toolkit (IoT Kit) deliver upgraded performance with lower power, enhanced media & AI capabilities, and IoT-centric features. These leading-edge technologies and developer tools enable Intel, Convergent, and

their ecosystem partners to more securely build and deploy solutions at scale that enable physical security and AI use cases seamlessly from edge to cloud. Within these solutions—built on available technology and ready for implementation today—several example use case scenarios provide a real-world view of comprehensive virtual security guard tools.

These tools, when strategically developed for an organization's unique needs and combined with physical security guards wherever they are required, can improve a business's security posture, leveraging operational optimization to facilitate the management of both costs and risks in the process.

## Use Case Scenarios for Implementation of Virtual Security Guard Tools

### Situational Monitoring

- Video Security
- Video Forensic Analysis
- Trespassing detection
- Unusual Behavior Detection
- Weapon detection in public areas
- Radars/lidars
- Event Monitoring
- Thermal Imaging & Anomaly Detection
- Fire/Explosion detection
- Leak Detection (gas/contaminants)
- Perimeter Tracking
- Boundary monitoring
- Vehicles monitoring
- Intrusion detection
- License Plate Recognition
- Crowd tracking
- Traffic flow optimization

- Queue management
- Accident detection
- Access control
- Smoke detection
- Missing object detection

### Environmental Monitoring

- Monitoring of humidity, air quality in of public city space
- Monitoring of CO2, CO, natural gases in various environments
- Environmental Temperature Monitoring

### Interactive Media

- Consumer/Product Information
- Self-Check-In and Out
- Remote Expert
- Transaction Processing
- Guest Experience
- Virtual City Concierge

- Interactive Content
- Wayfinding
- Smart Emergency ID's
- Self-Service Government (DMV)
- Operations Centers
- Ticket Dispensing
- Advertising & Brand Promotion
- Product matching
- Crowd prediction
- Payment authorization
- Service standard monitoring (Associate responsiveness monitoring/assessment)
- Customer traffic analysis (Dwell time)
- Inventory level monitoring
- Guest profiling
- POS auto checkout
- Personalized offers
- Shopper tracking

# Getting Started

## Starting point for digital transformation journey:

Given the broad array of technologies, market trends, digital transformation initiatives, and more that are applicable to generating a virtual guard security experience across a broad spectrum of industries, we ask interested enterprises to consider a phased approach that represents a manageable, approachable way to implement and maintain a virtual security guard experience, starting today.

### Phase 1

Layering the traditional physical security/access control implementation with intelligent and connected infrastructure to act as a basis for the virtual security guard experience (i.e., Convergent's Cloud Services Platform).

### Phase 2

Implementing larger-scale, commercially available capabilities that address the security challenges/risks that your organization, with the support of Convergent and Intel, identifies as being readily deployable and "most critical" (i.e., visitor management/wayfinding kiosks, smart parking, mobile credentialing, etc.)

### Phase 3

Identify the additional capabilities/ecosystem partners required to close the technology capability gaps for a given customer or industry in order to achieve a total virtual security guard experience (i.e., specific Computer Vision AI workloads, robots, drones, etc.)

### Phase 4

Conduct an iterative process to continuously learn from and improve upon the evolving virtual security guard experience.

Convergent and Intel believe organization leaders can successfully transform their security operations by establishing clear business goals and KPIs, undergoing operational analysis, creating detailed workflows and functional designs, building a technology roadmap and establishing priorities, justifying business expenses and defining value, and then implementing a plan in phases with short- and long-term success factors. Continued design optimization can further increase implementation effectiveness over time (i.e., new solutions, improved AI models, faster processing power, etc.).

## Explore more

Explore more about Convergent solutions powered by Intel® technology by contacting us today:

**Convergent Sales:** [sales@convergent.com](mailto:sales@convergent.com)

**Intel Sales:** Will Stewart, Edge Partner Sales, Digital Safety & Security/Video, Intel



## Endnotes

1 [BLS Info on Security Guards](#)

2 [BLS Info on Security Guards](#)

3 [Progressive Automations](#)

4 [Labor Market Info](#)

5 Services Employees International Union (nation's largest private security officers' union) via [Guard Systems Inc.](#)  
[IBM Security and the Ponemon Institute](#)



## Notices & Disclaimers

Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel's [HYPERLINK "https://www.intel.com/content/www/us/en/policy/policy-human-rights.html"](https://www.intel.com/content/www/us/en/policy/policy-human-rights.html) Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

February 2022

# Think big

Assess all the ways technology  
can facilitate meaningful change

# Start small

Get going with projects and opportunities

# Move fast

Learn, adjust, iterate

The Intel logo, consisting of the word "intel" in a lowercase, sans-serif font, is centered within a white square. The background of the entire slide is a dark blue field filled with a complex network of glowing blue and white lines, dots, and geometric shapes, suggesting a digital or technological theme.

convergent<sup>®</sup>