

Security Guards

AI and robotics fundamentally restructuring monitoring, access control, and patrol duties for guards.

EXPOSURE	WINDOW	ADOPTION TODAY	READING
55 Elevated exposure	2–5 yrs until change lands	High	The role is being reshaped. Exposure is the share of today's work AI can plausibly take on within the window.

§ 01WHAT IS HAPPENING

What is happening to security guards

Impact

AI tools and robotic systems are autonomously monitoring surveillance feeds, detecting anomalies, managing access points, and performing basic patrols. This compels Security Guards to radically pivot towards overseeing automated systems, troubleshooting technology, managing complex human interactions, and providing indispensable intervention in high-risk scenarios.

Risk

Radical role overhaul; pervasive automation leading to significant job displacement and specialized human focus.

The Security Guard role faces profound and accelerating redefinition by AI and robotics. AI will assume command of vast routine monitoring tasks, basic access control, and predictable patrols. Security Guards must immediately pivot to becoming experts in leveraging AI and robotic systems for hyper-efficiency and enhanced situational awareness, intensely validating AI outputs for accuracy and safety, and dedicating their expertise to the irreplaceable human elements of the role: profound judgment in ambiguous threats, nuanced de-escalation, and critical ethical decision-making regarding public safety and privacy in an increasingly automated environment.

Sector readiness

Rapid & Transformative Integration

The security, surveillance, and property management sectors are aggressively integrating AI and robotics, driven by overwhelming demand for efficiency, real-time threat detection, and comprehensive coverage. AI is rapidly moving beyond pilot stages to widespread adoption for monitoring, access control, and patrol, fundamentally altering traditional workflows and competitive dynamics.

§ 02 POSITION

Where you stand

- i The Security Guard role is undergoing a profound and accelerating redefinition by AI and robotics, fundamentally restructuring monitoring, access control, and patrol duties.
- ii AI will autonomously manage vast routine tasks, optimize surveillance, and streamline access, compelling Guards to pivot to indispensable oversight, complex human interaction, and profound ethical judgment.
- iii Survival and impact will hinge on Security Guards mastering AI and robotic tools, critically validating AI outputs for safety, championing ethical AI, and providing irreplaceable human vigilance and de-escalation at the heart of public safety.

§ 03 ACTIONS

15 POINTS

What this means for you

Concrete changes to how the work gets done, in the order you are likely to meet them.

- 01 **AI-Driven Autonomous Surveillance Monitoring.** Security Guards will oversee AI-powered CCTV systems that autonomously monitor vast camera feeds, identifying suspicious activities, detecting unauthorized access, and flagging anomalies (e.g., unattended bags, unusual gatherings) in real-time. This radically frees guards from constant screen vigilance, demanding focus on human intervention.
- 02 **AI-Powered Predictive Threat Detection.** Security Guards will leverage AI models that autonomously analyze historical incident data, environmental factors, and behavioral patterns to predict potential security breaches, theft attempts, or violent incidents before they occur. This enables proactive deterrence and targeted deployment of human guards.
- 03 **Automated Access Control & Biometric Verification.** AI tools will autonomously manage access points via facial recognition, fingerprint scans, or gait analysis. Security Guards will primarily oversee these autonomous systems, intervening for exceptions, verifying identities for high-security areas, and managing visitor flow.

-
- 04 **Robotic Patrols & Autonomous Security Vehicles.** Security Guards will oversee fleets of AI-powered autonomous patrol robots or drones that autonomously conduct routine patrols, monitor perimeters, and respond to basic alerts. Their role will shift to managing robot routes, resolving navigation issues, and responding to critical incidents flagged by robots.
-
- 05 **Generative AI for Incident Reports & Communication.** AI can autonomously draft initial versions of incident reports, daily logs, and security alerts based on verbal inputs or detected events. This streamlines documentation, ensuring consistency and allowing Security Guards to focus on immediate response and clear communication.
-
- 06 **Focus on Nuanced Human Interaction & De-escalation.** As AI assumes command of routine monitoring and physical patrols, the paramount value of Security Guards will be their irreplaceable human ability to engage with individuals, de-escalate conflicts, provide empathetic assistance in emergencies, and manage complex social dynamics with profound judgment.
-
- 07 **AI for Anomaly Detection in Behavior.** AI vision systems are autonomously analyzing human movement and behavior for patterns that deviate from normal. Security Guards will interpret AI-flagged anomalies (e.g., loitering, unusual carrying of objects) to determine if a human intervention is needed.
-
- 08 **Ethical AI in Surveillance & Privacy.** Security Guards will bear profound responsibility for auditing AI surveillance systems for algorithmic bias (e.g., racial bias in facial recognition), ensuring data privacy for individuals, and upholding ethical standards for monitoring public and private spaces.
-
- 09 **Human-AI Teaming for Enhanced Response.** Security Guards will operate in seamless human-AI teams. AI will provide real-time alerts, visual analytics, and risk assessments, while the human guard leads physical intervention, applies nuanced judgment in ambiguous situations, and manages critical ethical decisions.
-
- 10 **AI-Driven Alarm Monitoring & Triage.** AI systems will autonomously monitor vast streams of alarm data (e.g., motion sensors, door contacts), filter out false positives, and prioritize legitimate threats. Security Guards will focus on validating AI-triaged alarms and responding to actual incidents.
-
- 11 **Continuous Learning & Security Tech Literacy.** The exponential pace of AI integration in security demands that Security Guards commit to continuous, aggressive learning of new AI-powered surveillance systems, robotic patrols, and advanced analytics platforms, as a foundational competency for effective security operations.
-
- 12 **Specialization in AI-Integrated Security Operations.** The field will see a rise in Security Guards specializing in managing and optimizing AI-driven security control rooms, troubleshooting AI system issues, and training other staff on new AI-powered security technologies.
-
- 13 **AI for Predictive Maintenance of Security Systems.** AI models will autonomously analyze sensor data from security cameras, access control systems, and alarms to predict equipment failures. This enables proactive maintenance, ensuring continuous operation of critical security infrastructure.
-
- 14 **Leadership in Security Transformation.** Security Guards in leadership roles will play a crucial role in guiding their teams and organizations through the pervasive adoption of AI, advocating for strategic AI solutions, and fundamentally reshaping the future of physical security.
-

15 **Strategic Public Interaction & Trust Building.** As AI streamlines operational tasks, Security Guards will dedicate more time to fostering profound relationships with the public, building trust within communities, and acting as visible, reassuring presences in the spaces they protect.

What is pushing this change

- 01 **High Volume of Routine Monitoring Tasks.** Monitoring vast numbers of cameras, entry points, and alarms is highly repetitive and error-prone for humans, making AI ideal.
- 02 **Advancements in AI/ML (Computer Vision, Predictive Analytics, Robotics).** Breakthroughs in AI fields enable sophisticated image analysis, autonomous movement, and intelligent anomaly detection for security.
- 03 **Urgent Demand for Real-time Threat Detection.** Organizations require instant alerts for threats, minimizing response time to security incidents.
- 04 **Critical Shortage of Security Personnel.** The severe global shortage of security guards compels aggressive AI and robotics adoption to augment human capacity.
- 05 **Relentless Pressure for Cost Optimization.** AI automation of monitoring, patrols, and access control drives aggressive security cost reductions.
- 06 **Complexity of Large-Scale Security Environments.** Managing security across large campuses, multiple buildings, or complex industrial sites benefits from AI-powered oversight.
- 07 **Growth of IoT Sensors & Smart Security Systems.** The proliferation of smart cameras, access control systems, and environmental sensors provides rich input for AI analysis.
- 08 **Demand for Proactive & Predictive Security.** Organizations seek to prevent security incidents before they occur, rather than just react to them, which AI can enable.
- 09 **Focus on Data-Driven Security Decisions.** AI provides objective, data-driven insights into security vulnerabilities and operational efficiency.
- 10 **Ethical Concerns & Public Scrutiny.** AI's use in surveillance and automated decision-making raises significant privacy and bias concerns, leading to public scrutiny.

Impact by sector

The headline figure is an average. Where you work changes the picture.

Control Room Operators (Security)	AI for autonomous CCTV monitoring, alert triage, and incident detection. Focus on rapid analysis and dispatch of human responders.
Patrol Guards (Physical)	AI for autonomous patrols, perimeter monitoring (drones), and basic incident response. Focus on responding to AI-flagged alerts.
Access Control Guards	AI for autonomous biometric verification, visitor management, and automated entry/exit. Focus on high-value identity verification and exceptions.
Loss Prevention Officers (Retail)	AI for autonomous analysis of surveillance footage (theft patterns) and transaction data. Focus on investigating complex fraud and internal theft.
Chief Security Officers (CSOs)	AI for overall security strategy, risk assessment, and leading AI deployment across the enterprise. Focus on strategic leadership and governance.

Skills to build

The skills that keep the human part of this work valuable as the routine part is automated.

- 01 **Situational Awareness & Observation.** The ability to maintain a clear mental picture of a security situation, observe subtle cues, and interpret complex real-time data.
- 02 **AI/Security Tech Literacy & Oversight.** Proficiency in using AI-powered CCTV analytics, autonomous patrol robots, access control systems, and other security tech, and interpreting AI alerts.
- 03 **De-escalation & Conflict Resolution.** Skill in calming tense situations, active listening, and effectively managing conflicts or aggressive individuals peacefully.
- 04 **Physical Intervention & Restraint (if applicable).** Mastery of techniques for safe physical intervention, if required, for individuals who pose a threat (applies where authorized).
- 05 **Ethical AI Use & Privacy.** Upholding the highest standards of individual privacy, understanding potential biases in AI surveillance, and ensuring ethical AI deployment in security.
- 06 **Problem-Solving & Critical Judgment.** The ability to rapidly assess ambiguous threats, diagnose root causes of security incidents, and make sound judgments under pressure.

- 07 **Communication & Incident Reporting.** Clearly and concisely communicating security incidents, AI-generated insights, and response actions to colleagues, law enforcement, and management.
- 08 **Adaptability & Stress Management.** Maintaining composure and decisive action in high-stress, rapidly evolving security situations, and adapting to unforeseen circumstances.

§ 07 INSTRUMENTS

12 ENTRIES

Tools in use

KINDS OF TOOL WORTH KNOWING

- 01 **AI-Powered Video Analytics & Surveillance.** Software that uses AI to autonomously analyze video feeds for anomaly detection, object recognition, behavior analysis, and threat identification.
- 02 **AI for Access Control & Biometric Systems.** Systems that leverage AI for facial recognition, fingerprint scanning, and other biometrics to autonomously manage access points and visitor authentication.
- 03 **Autonomous Security Robots & Drones.** Unmanned ground vehicles (UGVs) and aerial vehicles (UAVs) that use AI for autonomous patrols, perimeter monitoring, and basic incident response.
- 04 **AI for Predictive Policing (Security Focus).** AI models that autonomously analyze historical crime data, security incidents, and environmental factors to predict potential security hotspots or threats.
- 05 **AI for Security Orchestration, Automation, & Response (SOAR).** Software that automates security workflows, orchestrates security tools, and automates incident response playbooks using AI.
- 06 **Generative AI for Incident Reports.** Large Language Models (LLMs) used to autonomously draft initial versions of security incident reports, daily logs, and security alerts.

NAMED TOOLS ALREADY IN USE

- Verkada (AI Cameras) / Milestone Systems (VMS with AI)**

Leading providers of AI-powered video surveillance and analytics platforms for physical security.

VISIT
- Genetec (Security Center) / Suprema (Biometric Systems)**

Integrated security platforms that leverage AI for access control, video surveillance, and identity management.

VISIT
- Knightscope (Security Robots) / Boston Dynamics (Spot robot)**

Manufacturers of autonomous security robots and drones designed for patrols and monitoring in various environments.

VISIT
- GardaWorld (Predictive Policing Services) / Palantir Gotham (for security)**

Security service providers and data platforms that use AI for predictive policing and threat intelligence in physical security.

VISIT
- Palo Alto Networks Cortex XSOAR / Splunk SOAR (Phantom)**

Leading SOAR platforms that integrate AI for automated incident response and security orchestration.

VISIT

ChatGPT / Google Gemini (for security reports)

VISIT

Generative AI models that can autonomously draft various security-related documents, from incident reports to daily logs.

§ 08 EXAMPLES

5 EXAMPLES

In practice

Ways people in this role are already using AI, and what they get from it.

Automate Video Surveillance Monitoring

EXAMPLE 1

HOW

Security Guards will oversee AI-powered video analytics software that autonomously monitors hundreds of CCTV cameras. The AI will automatically detect suspicious behavior (e.g., loitering, unauthorized entry), unusual movements, or unattended objects, flagging them for human review and response.

GAIN

Significantly reduces manual monitoring fatigue, increases threat detection accuracy, and allows guards to focus on higher-value interventions.

Deploy Autonomous Patrol Robots

EXAMPLE 2

HOW

Security Guards will manage a fleet of AI-powered autonomous security robots (e.g., Knightscope) that conduct routine patrols of large properties. They will monitor the robot's sensor data, resolve navigation issues, and respond to critical alerts or incidents the robot flags.

GAIN

Extends patrol coverage, provides continuous monitoring in large areas, and frees human guards for more complex tasks.

Streamline Access Control with AI

EXAMPLE 3

HOW

Security Guards will oversee an AI-driven access control system. The AI will autonomously verify identities via facial recognition or biometrics for entry/exit, managing routine access. The guard intervenes for visitors, complex identity issues, or high-security area access.

GAIN

Automates routine entry/exit, enhances security verification, and allows guards to focus on managing visitor experience and high-risk individuals.

Generate Incident Reports

EXAMPLE 4

HOW

Security Guards can instruct a generative AI tool to draft an initial incident report after a security event. By providing key details, events, and observations, the AI will autonomously generate a structured report for the guard's refinement and submission.

GAIN

Saves significant administrative time, ensures consistent and detailed reporting, and allows guards to focus on immediate response.

Predict Security Threats

EXAMPLE 5

HOW

Security Guards will utilize an AI model that autonomously analyzes historical incident data, environmental factors (e.g., time of day, day of week), and real-time surveillance feeds. The AI will predict potential security threats (e.g., theft, trespassing) in specific areas, guiding proactive patrols.

GAIN

Enables proactive security measures, optimizes resource deployment, and strengthens overall security posture by anticipating threats.

§ 09 CONTEXT

How this role compares

Three neighbouring roles chosen to show the direction of travel.

Surveillance Monitors
(Routine screen watch-
ing) / Access Control
Booth Operators (Basic
ID checks)

MORE EXPOSED

AI IMPACT

Catastrophic (AI can autonomously monitor CCTV feeds; AI can au-
tonomously verify IDs and grant basic access.)

WORK MOVES TO

Immediate need for radical re-skilling into AI oversight, troubleshooting
automated systems, or specialization in complex human interaction.

Robotics Engineers (Se-
curity) / AI Computer Vi-
sion Engineers (Security)

DIFFERENT SKILLS, GROWING

AI IMPACT

Foundational (They design and build the AI algorithms and robotic
systems that power automated security and surveillance.)

WORK MOVES TO

Deep expertise in AI/ML algorithms, computer vision, robotics, and
software engineering, with a focus on security applications.

Police Officers (Active
law enforcement) / Crisis
Negotiators (High-stakes
human interaction)

COMPLEMENTARY, LESS EXPOSED

AI IMPACT

Low-Moderate Augmentation (AI assists in data for police; AI provides
background for negotiators), but core law enforcement authority, direct
physical intervention, and nuanced human influence remain para-
mount.

WORK MOVES TO

Law enforcement, crime investigation, and physical intervention (Po-
lice Officers); High-stakes negotiation, emotional intelligence, and
de-escalation expertise (Crisis Negotiators).

§ 10 VERDICT

Closing judgement

For Security Guards, AI and robotics are not merely tools but a radical force of transformation that will fundamentally redefine their role. It will autonomously handle the mundane, amplify surveillance, and streamline access, compelling guards to pivot to indispensable oversight, complex human interaction, and profound ethical judgment. The future Security Guard will be a visionary orchestrator of human-AI collaboration, providing irreplaceable vigilance and de-escalation at the heart of public safety.

Evidence and revisions

What the exposure figure rests on, what changed when it was last revised, and the published work cited for this role.

SCORE

70 to 55

WINDOW

1-4 years to 2-5 years

The 4 October 2026 review moved the score down by 15 points.

Microsoft's AI applicability score for the matching occupation is 0.14, in the lower half of 785 US occupations; Anthropic's observed-exposure data records almost no Claude usage on this occupation's tasks; the US Bureau of Labor Statistics places it in the 'moderate' AI-exposure tier; BLS projects employment to grow 0.9% over 2025–35. Blending our 2025 editorial figure (60%) with the 2026 evidence composite (40%) moves the score from 70 to 55 and lengthens the window from 1-4 years to 2-5 years.

MEASURES BEHIND THE SCORE

US Bureau of Labor Statistics · *Employment Projections 2025–35 and AI Exposure Categories* (27 August 2026)

AI-exposure tier: Moderate. Projected employment change 2025–35: +0.9%. Matched to Security guards.

PUBLISHER PDF ARCHIVED COPY

Microsoft Research · *Working with AI: Measuring the Applicability of Generative AI to Occupations* (10 July 2025)

AI applicability score 0.14 (percentile 48 of 785 occupations) for SOC 33-9032.

PUBLISHER PDF ARCHIVED COPY

Anthropic · *Anthropic Economic Index report: Cadences* (26 June 2026)

Observed exposure 0.00 for SOC 33-9032 (no meaningful Claude usage recorded on these tasks).

PUBLISHER PDF

World Economic Forum · *The Future of Jobs Report 2025* (7 January 2025)

Cashiers and ticket clerks head the WEF fastest-declining list; light-truck and delivery drivers are on the growing list.

PUBLISHER PDF

UK Department for Science, Innovation and Technology · *Assessment of AI capabilities and the impact on the UK labour market* (28 January 2026)

UK context: around 70% of UK workers are in occupations with tasks AI could perform or enhance, above the US average; a one-standard-deviation rise in exposure was associated with a 3.9% fall in UK job postings.

PUBLISHER ARCHIVED COPY

ALSO CITED FOR THIS ROLE

McKinsey Global Institute · *Agents, robots, and us: Skill partnerships in the age of AI* (25 November 2025)

Physical, in-person work sits mainly in the robot (not agent) share of technical potential, which McKinsey puts at roughly 13% of US hours and expects to move more slowly.

PUBLISHER

Archived copies are served only where the licence permits; otherwise the link goes to the publisher. Full research library: <https://www.careerguard.ai/sources>

§ 12 APPENDIX

Method and sources

Each report was written from a large body of published research and then, in October 2026, re-scored against occupation-level evidence: the US Bureau of Labor Statistics AI-exposure classification and 2025–35 projections, Microsoft Research’s AI applicability scores and Anthropic’s observed-exposure data, cross-checked against the reports listed in the Evidence section above. The organisations and publications below are the standing literature behind the narrative sections. Every source, with dates, licences and archived copies where we are permitted to hold them, is catalogued in the research library.

Scores are revised by blending the previous editorial figure (60%) with a composite of the three occupation-level measures (40%), capped at fifteen points per revision and rounded to the nearest five. The window shifts one notch when a score moves ten points or more. Hand adjustments are recorded with their reason in the revision log.

I GLOBAL AND MACROECONOMIC IMPACT OF AI ON WORK

World Economic Forum

The Future of Jobs Report series — Employer survey of expected job growth and decline, skill shifts and technology adoption (2020, 2023 and 2025 editions); *Artificial Intelligence and the Future of Entry-Level Work* (2026).

AI governance and transformation reports — Frameworks on ethical AI, talent strategy and industry transformation.

McKinsey Global Institute

AI, Automation and the Future of Work series — Research quantifying automation potential by task, sector and demographic, from "Jobs Lost, Jobs Gained" to "Agents, robots, and us" (2025).

Industry-specific reports — Financial services, healthcare, manufacturing and others.

PwC

Global AI Jobs Barometer — Annual analysis of job postings and productivity by AI exposure (2024–2026 editions).

Upskilling Hopes and Fears survey — Employee perceptions and readiness.

Microsoft Research and Anthropic

Working with AI (2025); *Anthropic Economic Index* (2025–2026) — Occupation-level usage data from Copilot and Claude conversations, the two observed-usage measures behind the 2026 revision.

Stanford Digital Economy Lab and Stanford HAI

Canaries in the Coal Mine? (2025–2026); AI Index Report (annual) — Payroll evidence on early-career employment in exposed occupations; annual measurement of AI capability, investment and adoption.

Deloitte

Human Capital Trends series — Workforce, talent and HR technology trends.

Tech Trends series — Emerging technologies and their business implications.

Accenture

Technology Vision series — Forward-looking analysis of emerging technology, with emphasis on AI.

Fjord Trends — Design, innovation and human experience in a digital world.

Boston Consulting Group

AI/ML insights and industry solutions — "The AI Revolution in the Workplace" and related research.

EY

AI and workforce reports — Adoption, talent strategy and ethics.

IBM Institute for Business Value

AI and automation studies — Business models, workforce evolution and leadership.

OECD

AI Policy Observatory — International data and policy on AI, labour markets and skills.

Employment Outlook — Labour-market trends including technological impact (2023–2026 editions).

International Labour Organization

Generative AI and Jobs: A Refined Global Index of Occupational Exposure (2025) — Task-level exposure gradients for every ISCO occupation; successor to the 2023 global index.

International Monetary Fund

Staff Discussion Notes on AI and work (2024, 2026) — Complementarity framing: where AI augments and where it substitutes.

UK Department for Science, Innovation and Technology

Assessment of AI capabilities and the impact on the UK labour market (2026) — UK occupational exposure and job-posting evidence.

Brookings Institution

AI and automation research — Economic and social implications, displacement and skills.

Yale Budget Lab and Goldman Sachs Research

Tracking the Impact of AI on the Labor Market; AI and the US labour market (2026) — Aggregate labour-market monitoring; macro displacement estimates.

Oxford University (Oxford Martin School)

The Future of Employment — Frey & Osborne and subsequent research on susceptibility to automation.

MIT Technology Review

AI & Work — Reporting on AI research and its implications for industries and jobs.

Gartner

Hype Cycle for Artificial Intelligence — Maturity and adoption of AI technologies.

Future of Work reports — Workplace models and talent strategy.

U.S. Bureau of Labor Statistics

Employment Projections 2025–35; AI Exposure Categories; Occupational Outlook Handbook — Ten-year employment projections and, from the 2025 cycle, an AI-exposure tier for every detailed occupation.

Indeed Hiring Lab

AI at Work Report (2025) and posting-market updates — Skill-level transformation estimates and job-posting trends by occupation.

II CORE AI AND MACHINE-LEARNING RESEARCH

OpenAI

Research papers, blog and API documentation — Large language models, generative AI, safety and societal impact.

Google DeepMind

Research papers and blog — Reinforcement learning, AI for science, AGI and ethics.

Meta AI

Research papers and blog — Large language models, computer vision, AI for social good.

Hugging Face

Transformers library and model hub — Open-source state-of-the-art NLP models.

TensorFlow and PyTorch

Documentation and community forums — Core frameworks illustrating practical capability.

arXiv

cs.AI, cs.LG, cs.CV, cs.CL — Pre-print research.

NeurIPS and ICML

Conference proceedings — Top-tier academic research.

ACM and IEEE

Journals and proceedings — ACM Computing Surveys; IEEE Transactions on AI.

Kaggle

Datasets and competition solutions — Applied machine learning on real-world problems.

The Alan Turing Institute

Research and reports — Responsible and applied AI.

III ETHICAL AND RESPONSIBLE AI DEPLOYMENT

NIST

AI Risk Management Framework — Voluntary framework for managing AI risk.

European Commission

AI Act — Risk-tiered legal framework for AI.

Ethics Guidelines for Trustworthy AI — Principles for responsible development.

Partnership on AI

Research and best practice — Responsible AI development.

AI Now Institute

Annual reports — Social implications: power, inequality, rights.

ACM FAccT

Proceedings — Fairness, accountability and transparency.

Data & Society

Publications — Social implications of data-centric technology.

WIPO

Conversation on IP and AI — Intellectual-property implications of AI.

IEEE Global Initiative on Ethics of AI/IS

Ethically Aligned Design — Recommendations for ethical AI design.

Center for AI and Digital Policy

Policy briefs — Accountable AI policy.

REPORT NO. 342 · SECURITY GUARDS · [WWW.CAREERGUARD.AI/REPORTS/SECURITY-GUARDS](https://www.careerguard.ai/reports/security-guards) · MARKDOWN AT /MD · FREE TO READ