Homeland Security And Emergency Management - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

Homeland Security And Emergency Management Market Analysis

The homeland security and emergency management market was valued at USD 3.82 billion in 2025 and is on track to reach USD 5.5 billion by 2030, reflecting a 7.56% CAGR. Intensifying overlaps between cyber, physical, and environmental threats motivate governments and private operators to invest in integrated platforms that merge perimeter protection with real-time digital intelligence. State-sponsored cyberattacks, rising geopolitical frictions, and more frequent climate-driven disasters are expanding the addressable scope of the homeland security and emergency management market, while emerging technologies such as 5G, cloud, and AI deliver the scale required for nationwide rollouts. Competitive intensity is growing as defense primes partner with cloud and telecom players to field modular solutions for critical infrastructure, public safety communications, and border management. At the same time, purchasing decisions are moving toward outcome-based contracts in which vendors must demonstrate faster incident response and measurable risk reduction. As procurement frameworks mature, regional differentiation is widening: North America adopts zero-trust cyber architectures, Asia accelerates smart-city surveillance deployments, and Europe mandates strict data-protection safeguards alongside cross-border intelligence sharing.

Global Homeland Security And Emergency Management Market Trends and Insights

Escalating State-Sponsored Cyberattacks on Critical Infrastructure

Nation-state groups have shifted from intelligence gathering to the placement of dormant malware within electric grids, ports, and

water systems. The FBI disclosed that Volt Typhoon maintained covert access to US transport networks for over five years and could launch disruptive actions during conflict events. Operators are therefore retiring perimeter-centric defenses in favor of zero-trust models that continuously validate every device and user. Energy utilities segment operational-technology networks, while airports apply behavioral analytics to spot suspicious lateral movement. These measures have pushed cybersecurity spending toward identity management, encrypted industrial protocols, and continuous network monitoring. As ransomware overlaps with geopolitically motivated sabotage, insurance premiums have risen, elevating the total cost of inaction and spurring additional safeguards.

Mandatory NG911 / EU-112 Public Warning System Compliance Deadlines

Regulatory calendars in the United States and European Union mandate next-generation emergency call routing, location precision under three meters, and multimedia exchange between dispatchers and first responders. Compliance projects require cloud-based call handling, redundant fiber backbones, and cybersecurity certification aligned with NIST and ETSI standards. Counties already upgraded report lower call abandonment rates and faster triage of multi-casualty events. Vendors supplying IP core services, geospatial analytics, and cyber-hardened radio gateways benefit directly, while system integrators capture extended maintenance contracts. Because public warning systems must interface with private telecom networks, cross-border standards are tightening, accelerating platform convergence across continents.

Fragmented Multi-Jurisdiction Procurement

Emergency agencies often buy radios, sensors, and analytics platforms under separate grant programs, creating incompatible data schemas obstructing mutual aid. The US Government Accountability Office estimates that eliminating duplicated homeland security contracts could save hundreds of millions. Parallel challenges surface in Europe, where municipal surveillance software can struggle to integrate with national border systems. Vendors must provide middleware that translates between proprietary formats, but the additional engineering cost slows rollout schedules and increases total project price, tempering near-term growth.

Other drivers and restraints analyzed in the detailed report include:

AI-Enabled Video Analytics Roll-outs in GCC and Asian Megacities / 5G Private Network Adoption Inside Military Bases / Litigation and Moratoria on Facial-Recognition Surveillance /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Critical infrastructure security generated the largest revenue slice in 2024, underscoring heightened concern over the resilience of electricity, water, and transportation assets. The segment's 21.52% homeland security and emergency management market share arose after publicized attempts to compromise rail signaling and pipeline monitoring networks. Utilities responded by segmenting supervisory control and data acquisition (SCADA) traffic, deploying intrusion detection at substations, and integrating incident-response playbooks with federal fusion centers. This segment's homeland security and emergency management market size is forecast to rise steadily on continued grant allocations, mandatory cyber incident reporting rules, and the incorporation of digital twins that enable predictive maintenance.

Although smaller in absolute terms, maritime and port security are projected to expand at 8.46% CAGR through 2030, reflecting the strategic value of seaborne trade lanes, NATO's Baltic Sentry drone flotilla, and commercial AI systems that flag vessels deviating from declared routes highlight a broader commitment to maritime domain awareness. Ports pair surface radars with

underwater acoustics to detect unauthorized divers near fiber cables. As insurance underwriters demand robust monitoring to cover sabotage risks, procurement of autonomous patrol boats and AI-scored risk dashboards accelerates. Additional growth drivers include decarbonization mandates that require new emission-tracking sensors, further widening the solution scope within the homeland security and emergency management market.

Other solution lines-CBRNE detection, perimeter protection, aviation security, and risk and emergency services-add redundancy across the threat spectrum. While their share fluctuates, integrated command-and-control platforms allow agencies to visualize alerts from all subsystems in a single pane, simplifying incident orchestration.

The Homeland Security and Emergency Management Market Report is Segmented by Solution Type (Critical Infrastructure Security, and More), Technology (AI and Machine Learning, and More), End-Use Vertical (Military and Defense, and More), and Geography (North America, Europe, and More). The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America led with a 36.81% share in 2024, supported by robust federal appropriations for critical-infrastructure defense and extensive collaboration between agencies and private operators. The Port of Los Angeles blocked 750 million hacking attempts in 2024, illustrating the attack volume shaping purchasing priorities. Zero-trust adoption rates outpace other regions, and grant frameworks such as the Infrastructure Investment and Jobs Act funnel funds toward resilience upgrades.

Asia-Pacific is the growth engine, expanding at 9.21% CAGR. Rapid urbanization and megacity investments create fertile ground for AI-enabled surveillance, smart evacuation corridors, and resilient telecom backbones. The 2024 Noto Peninsula earthquake exposed gaps in sensor coverage and spurred fast-track procurement of integrated warning platforms. Meanwhile, rising semiconductor fabs across Taiwan and South Korea require strict security perimeters and air-gap cyber defenses, intensifying regional spend.

Europe maintains a sizeable position through stringent regulatory mandates and joint border-management initiatives. Projects such as the biometric upgrade at Beirut-Rafic Hariri International Airport demonstrate the export of European standards beyond the continent. Funding from the EU Internal Security Fund underpins cross-border data-sharing hubs.

The Middle East continues to direct oil revenues toward layered airport, energy-facility, and public-venue protection systems. Africa and Latin America advance more slowly but prioritize maritime and disaster-response capabilities in coastal cities prone to hurricanes and cyclones.

List of Companies Covered in this Report:

Lockheed Martin Corporation / Northrop Grumman Corporation / RTX Corporation / General Dynamics Information Technology, Inc. (General Dynamics Corporation) / Thales Group / International Business Machines Corporation (IBM) / Honeywell International, Inc. / BAE Systems plc / Elbit Systems Ltd. / Cisco Systems, Inc. / Airbus SE / Leonardo S.p.A. / Booz Allen Hamilton, Inc. / Palantir Technologies Inc. / Fortinet, Inc. / Esri Global, Inc. / MOOG Inc. / AT&T Inc. / Accenture plc /

Additional Benefits:

 The market estimate (ME) sheet in Excel format /
3 months of analyst support /

Table of Contents:

SCOTTS INTERNATIONAL

Homeland Security And Emergency Management - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-22
		Signature