everbridge™

2026

Regional threat assessment

Geographic trends shaping the global security landscape

Table of contents

Foreword

As we look to the future, organizations are entering an era where risks that lead to vulnerabilities and operational disruptions are no longer sporadic; they are constant. Over the past few years, we've witnessed a fundamental shift in how risks emerge, cascade, and challenge resilience. What once seemed like distinct categories of risk, whether that be geopolitical, environmental, cyber, and violent extremism, are now converging into a complex, interconnected threat landscape. The risks of today are increasingly compounding into greater vulnerabilities for the future.

This year's threat assessment is not a simple report of isolated incidents or past events. It aims to provide insight into how these risks interact in ways that will disrupt continuity, safety, and stability at the organizational level. Proactive intelligence is no longer a luxury in building resilience; it's an absolute necessity.

Our analysis will examine each region worldwide, offering forward-looking assessments of the most relevant threats in each area. These aren't always the most obvious risks but are the ones our regional subject matter experts have identified as having the greatest organizational impact in the coming year. We'll also outline actionable strategies to get ahead of these threats and mitigate them, improving your organization's risk posture.

While the report will get into specifics, we do expect there to be major cascading risks from the geopolitical landscape, the growing threat of cyber threat actors, continued climate risk, and the difficulty to detect and prepare for risk presented by violent extremists.

Geopolitically, the global landscape is as uneasy as it's ever been, and long-standing alliances are being tested. From the Russia-Ukraine conflict and ongoing tensions in the Middle East to trade disputes and tariffs, these pressures have triggered economic instability, disrupted energy and food supply chains, and impacted information operations. For global enterprises, this means exposure not only in known hotspots but also in previously stable regions where political volatility now poses new challenges.

Climate risk is no longer a distant concern; it's an immediate operational challenge. The acceleration of extreme weather events strain infrastructure, displaces populations, and disrupts critical supply chains. For organizations, this creates acute disruptions, energy challenges, insurance volatility, and new compliance obligations tied to climate resilience and reporting.

The cyber threat landscape remains as dynamic and dangerous as ever. Threat actors, from nation-states to criminal groups, are leveraging increased coordination, precision,

and strategic intent. Ransomware, AI-driven deepfakes, disinformation campaigns, DDoS (distributed denial of service) attacks, and ICS (industrial control systems) targeting malware are no longer isolated incidents, but parts of broader campaigns with the potential to cause massive operational losses, or even physical impacts.

Violent extremism is also entering a new phase. Ideologically driven threats are no longer confined to fringe actors or isolated geographies. These threats are hard to detect, easy to conduct, and can be executed with minimal planning and funding. From politically fueled unrest in major cities to targeted attacks on infrastructure and individuals, the scope of these threats has expanded across both motivations and tradecraft. The strategic concern is not merely frequency, but the unpredictable nature of the threat.

What does this mean for organizations? It means risk management must evolve. Risk avoidance is no longer viable, nor is it the right approach. Organizations must focus on flexibility, deliberate risk assessment, and precise prioritization of mitigation strategies to limit impact. The speed at which an organization can anticipate, assess, and adapt to threats now represents a critical competitive advantage. It requires prioritization and flexibility, but also strategic, proactive intelligence, exercising, business continuity, and decisive decision making.

In 2026 and beyond, business continuity will increasingly depend on the ability to act on intelligence before risks become disruptions. While the challenges outlined in this report are significant, they can be navigated with the right approach. Success depends on your organization treating intelligence as a strategic asset and resilience as an enterprise-wide mandate.

Adam DeLuca
Director, Risk Intelligence, Everbridge

How to use this report

This document is intended to serve as a global framing and decision-support tool. It provides a comparative view of the geographic trends most likely to shape organizational risk in 2026, helping leaders understand where threats are intensifying, how they are evolving, and what types of disruption they are most likely to produce.

The report is divided into six geographic sections, each accompanied by a detailed, region-specific assessment published alongside this global overview. These companion documents delve deeper into regional dynamics, providing expanded analysis, detailed scenario planning, and actionable operational insights tailored to each area.

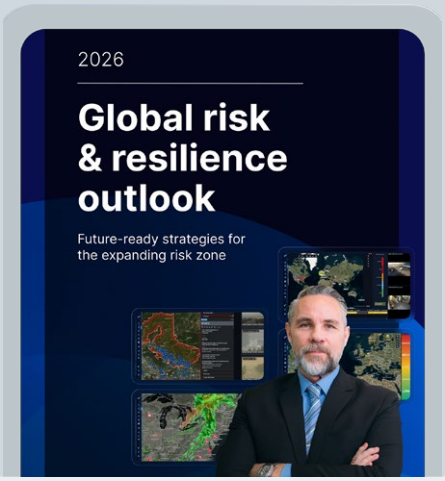
This report is designed to help you:

- Equip leadership teams with insights into the most significant regional risks expected to shape 2026.
- Identify vulnerabilities across sites, personnel, suppliers, travel, and critical dependencies.
- Focus your planning efforts by comparing risk drivers across regions and pinpointing areas where disruptions could cause cascading effects.
- Explore additional context and insights into specific regional risks by accessing more detailed analyses through the linked companion reports.

Each section of this report features a direct link to the full regional report, providing easy access to more detailed information.

In addition to these regional insights, Everbridge offers a broader perspective through our **2026 Global risk & resilience outlook**. While our regional assessments focus on local dynamics, the companion outlook identifies the top 10 global threats, ranging from AI-driven disruptions to supply chain shocks, and provides a strategic five-stage framework for building organizational resilience. The outlook combines global survey insights with actionable advice to help you protect your assets and maintain continuity in an increasingly interconnected landscape.

Access the 2026 Global risk & resilience outlook now →



North America overview

North America's 2026 risk environment is shaped by domestic polarization, policy volatility, and the accelerating convergence of cyber and physical threats. In the United States and Canada, domestic extremism remains a persistent concern - often decentralized and fueled by rapid online mobilization - contributing to elevated risk of lone-actor violence, targeted intimidation, and cyber-enabled harassment such as doxxing and swatting. These dynamics can reduce warning time and expand exposure beyond government targets, to include corporate leaders, public-facing facilities, and critical infrastructure.

Governance and policy uncertainty also loom large. In the United States, debates over federal authority, regulatory scope, and election administration continue to create uneven policy conditions across jurisdictions. Leadership turnover, court decisions affecting regulatory power, and intergovernmental friction increase the likelihood of administrative delays and inconsistent enforcement. These challenges complicate compliance and long-term planning for organizations operating across multiple states.

Economic and trade-policy volatility further adds to the risk picture. Tariff uncertainty, including potential legal and political challenges, creates planning difficulties for the manufacturing, technology, and consumer goods sectors. This is especially true for companies that rely on globally sourced materials. These pressures interact with elevated borrowing costs, which constrain organizations' ability to absorb sudden cost shifts or rapidly restructure supply chains.

At the same time, organizations face an increasingly complex cyber landscape. Threat actors are using automation and generative AI to increase the speed and scale of attacks. The growing dependence on energy-intensive data centers and AI-enabled processes heightens exposure to grid strain and power reliability issues, especially in regions where climate extremes also stress aging infrastructure.

What this means for organizations

Organizations should plan for limited warning time and compound disruption, where political volatility, digital threats, and infrastructure stress amplify each other. Priorities include strengthening protective intelligence for executives and facilities, maintaining flexible compliance and policy-tracking capabilities across jurisdictions, hardening cyber and identity controls against AI-accelerated threats, and stress-testing continuity plans for power instability and cyber–physical spillover.

Learn more

For expanded analysis, key scenarios, and preparedness considerations across the United States and Canada, access the North America regional threat assessment.

Europe overview

Europe enters 2026 facing sustained strategic pressure driven by geopolitics, climate stress, and internal social dynamics. The war in Ukraine continues to shape the security environment not only through conventional military activity, but also through persistent hybrid pressure. Cyber operations, sabotage, disinformation, and interference with energy and communications systems are likely to remain defining features of the threat landscape, particularly for EU and NATO member states.

Critical infrastructure, including power grids, undersea cables, transport corridors, and energy generation assets, remains a focal point for both state and non-state actors. Even limited disruption or "partial degradation" can produce cascading effects across energy markets, cloud services, finance, and communications. Defense-adjacent industries face additional exposure through cyber intrusion, supply-chain compromise, and information operations aimed at undermining production timelines and eroding trust.

Domestic factors also contribute to elevated risk. Protest and strike activity, particularly in countries facing fiscal constraints and electoral dynamics, is likely to remain episodic but high-impact. Transport networks are especially vulnerable, as localized interference can propagate quickly through interconnected rail, aviation, and freight systems.

Terrorism risk is expected to remain characterized by low-tech, lone-actor attacks against soft targets. This will lead to episodic spikes around major events that concentrate crowds and media attention, including the Milano–Cortina Winter Olympics and other high-profile gatherings. Meanwhile, climate stress, especially extreme heat and drought, functions as a recurring systems test, straining power generation, workforce capacity, and continental logistics.

What this means for organizations

Organizations should plan for intermittent but consequential disruption, rather than singular crises. Focus areas include resilience against cyber and sabotage pressure on critical dependencies, planning for transport unreliability and protest-linked interference, strengthening event and crowd-risk procedures for high-footfall locations, and integrating heat/drought thresholds into continuity and workforce planning.

Learn more

For country-level risk drivers, scenario detail, and operational planning guidance, access the Europe regional threat assessment.

Asia-Pacific overview

The Asia-Pacific region in 2026 is defined by strategic competition, climate vulnerability, and digitally mediated social change. In East Asia, the China–Taiwan–Japan corridor remains a focal point for layered disruption risk. Military signaling, repeatable blockade-style exercises, and sustained cyber activity create an environment where disruption can be scaled up or down without crossing traditional conflict thresholds, driving uncertainty across maritime and air routing, supply availability, and cross-border mobility.

In Southeast Asia, high-contact maritime coercion in the South China Sea continues to generate an “incident economy” of delays, insurance volatility, and compliance risk, particularly along the Philippines-facing frontline where frequent close encounters increase the risk of accident-driven escalation. These dynamics can tighten operating assumptions with limited notice, even absent open conflict.

Climate-driven disruption is another defining feature. Storm clustering has reduced recovery windows and left logistics corridors more fragile entering 2026. In this context, even moderate events can trigger outsized disruption due to degraded infrastructure and cumulative stress.

Social and political dynamics add further complexity. Youth-led mobilization, amplified through digital platforms, increasingly intersects with assertive digital governance measures. Platform restrictions, data demands, feature-level throttling, and licensing actions - often deployed during politically sensitive moments - can directly affect communications, payments, workforce coordination, and reputational management.

What this means for organizations

Organizations should prepare for repeatable, short-notice disruption across logistics, travel, digital services, and regulatory conditions. Resilience planning should emphasize trigger-based decision frameworks, alternate routing and supplier options, platform and communications redundancy, and the ability to operate through degraded connectivity and information reliability.

Learn more

For corridor-specific risk detail, country-level dynamics, and continuity considerations across the region, access the Asia-Pacific regional threat assessment.

Middle East and North Africa overview

The Middle East and North Africa enter 2026 with unresolved conflicts, shifting power balances, and mounting economic pressure. Escalation risk remains elevated across multiple theaters. In South Asia's western periphery, cross-border militancy and interstate friction keep the Afghanistan–Pakistan–India triangle volatile. In the Levant, Israel faces an election year amid unfinished conflicts with Iran and its proxy network, creating continued risk of renewed escalation affecting airspace, maritime routes, and critical infrastructure.

Across the Gulf, a firmer but more transactional U.S. security umbrella provides deterrence while testing the sustainability of the Gulf Cooperation Council (GCC) states' economic models. High defense spending, ambitious diversification agendas, and vulnerability to oil price fluctuations create a complex mix of opportunity and contingent risk, particularly when fiscal pressure intersects with security flare-ups.

Turkey presents a different profile, combining political pressure on opposition actors, economic fragility, and a tentative Kurdish peace track. Protest cycles, currency volatility, and governance uncertainty increase the likelihood of localized disruption in major urban centers.

Iran remains a dual-risk environment, facing both internal instability and potential external escalation. Fiscal strain, water shortages, and subsidy reforms increase the likelihood of protest activity and internet restrictions, while nuclear brinkmanship and asymmetric operations raise regional risk. In Lebanon, Syria, and Iraq, state authority remains contested by militias, creating a high-friction corridor where stabilization efforts coexist with persistent risk of episodic violence.

What this means for organizations

Organizations should plan for layered risk that combines security escalation, political disruption, and economic tightening. Key priorities include airspace and maritime contingency planning, cyber readiness during periods of escalation, workforce protection and movement planning in high-tension metros, and contractual/financial flexibility in environments where payment, tax, and regulatory conditions can shift quickly.

Learn more

For escalation scenarios, country-level analysis, and operational planning guidance across the region, access the Middle East and North Africa regional threat assessment.

Latin America and Caribbean overview

In Latin America and the Caribbean, 2026 risk is shaped by organized crime, political volatility, and rising compliance and enforcement pressure. Around Venezuela, heightened U.S.–Venezuela friction is driving airspace advisories, maritime interdiction risk, and insurance volatility that can affect wider Caribbean and northern South America routing and logistics. “Gray zone” pressure - rather than a single dramatic confrontation - remains the most likely operating pattern.

Mexico’s security environment is becoming more violent and legally consequential. Criminal groups continue to innovate tactically, including greater use of drones and intimidation along key industrial corridors. Moreover, terrorist designations and expanded sanctions enforcement increase compliance exposure for companies operating through vendors, logistics intermediaries, and local services in environments where coercion and extortion are common.

Brazil faces an expanding criminal footprint linking remote extractive economies to urban infrastructure disruption and port-related risk. Large-scale enforcement operations and gang retaliation can disrupt highways, commuter corridors, and logistics access with limited notice. Peru’s risk picture similarly reflects the overlap of crime and governance fragility, with urban extortion and illegal mining violence driving episodic disruption and periodic emergency measures.

Across the region, digitally driven youth mobilization is increasingly capable of scaling rapidly and concentrating disruption in government districts, landmark spaces, and major transport arteries - compressing warning time and complicating workforce mobility.

What this means for organizations

Organizations should anticipate corridor-specific disruption driven by crime, enforcement actions, and protest dynamics. Effective mitigation includes enhanced due diligence and vendor controls, secure routing and journey management, flexible staffing and remote-work triggers, and preparedness for sudden access constraints affecting downtown districts and logistics routes.

Learn more

For deeper country and corridor analysis, including compliance considerations and continuity planning guidance, access the Latin America and Caribbean regional threat assessment.

Sub-Saharan Africa overview

Sub-Saharan Africa enters 2026 with elevated political and security risk driven by dense election cycles, coup dynamics, militant insurgencies, and protracted conflicts. In parts of West Africa, coups and authoritarian consolidation continue to reshape governance, security partnerships, and regulatory conditions - often increasing volatility for organizations navigating licensing, payments, and reputational exposure.

Militant Islamist networks across the Sahel and Lake Chad Basin are expanding their reach, converging with criminal economies, and adapting tactically, including through the growing use of drones and kidnapping-for-ransom models. These dynamics elevate risk across energy, mining, logistics, education, and humanitarian sectors.

Sudan's civil war remains deeply destabilizing, with territorial fragmentation, mass displacement, and spillover into South Sudan and neighboring states. In eastern Democratic Republic of the Congo, the M23 rebel group's consolidation of territory and influence over mineral corridors introduces significant ESG, compliance, and supply-chain risk for industries reliant on cobalt, coltan, and related inputs. In the Horn of Africa, internal fragmentation and rising interstate tensions, including between Ethiopia and Eritrea, raise the potential for corridor disruption and regional contagion effects.

What this means for organizations

Organizations should plan for episodic, but potentially severe disruption tied to elections, conflict escalation, and insurgent activity, often accompanied by curfews, checkpoints, internet restrictions, and rapid shifts in authority. Key priorities include strengthened duty-of-care procedures, supply-chain diversification, political-risk monitoring around electoral milestones, and readiness for sanctions and compliance changes.

Learn more

For detailed sub-regional analysis, conflict scenarios, and operational risk guidance, access the Sub-Saharan Africa regional threat assessment.

Conclusion

The 2026 global security landscape is defined by convergence, complexity, and compressed warning time. Across regions, organizations face a world in which geopolitical competition, climate stress, technological change, and social polarization interact to produce non-linear disruption. Few risks exist in isolation, and even localized events can cascade across borders, sectors, and systems.

This assessment underscores a central insight: resilience in 2026 is not about predicting every threat, but about building the capacity to anticipate patterns, absorb shocks, and adapt quickly. Organizations that treat intelligence as a strategic asset, integrate risk across traditional silos, and plan for disruption as a recurring condition, will be better positioned to protect their people, operations, and reputations.

As the trends outlined in this report demonstrate, the challenge is significant, but it is navigable. With disciplined preparation, flexible response frameworks, and sustained investment in resilience, organizations can operate with confidence even in an increasingly uncertain world.

Everbridge High Velocity CEM™, powered by Purpose-built AI, is designed to meet the demands of this increasingly complex and interconnected world. Through intelligent automation, real-time risk intelligence, and a unified platform architecture, it empowers organizations to filter out operational noise, accelerate response times, and maintain operational continuity. Trusted by over 6,500 customers worldwide, Everbridge delivers scalable, enterprise-grade solutions that enable businesses to anticipate risks, adapt to disruptions, and thrive in an unpredictable global landscape.

Stay ahead of the expanding risk zone with Everbridge

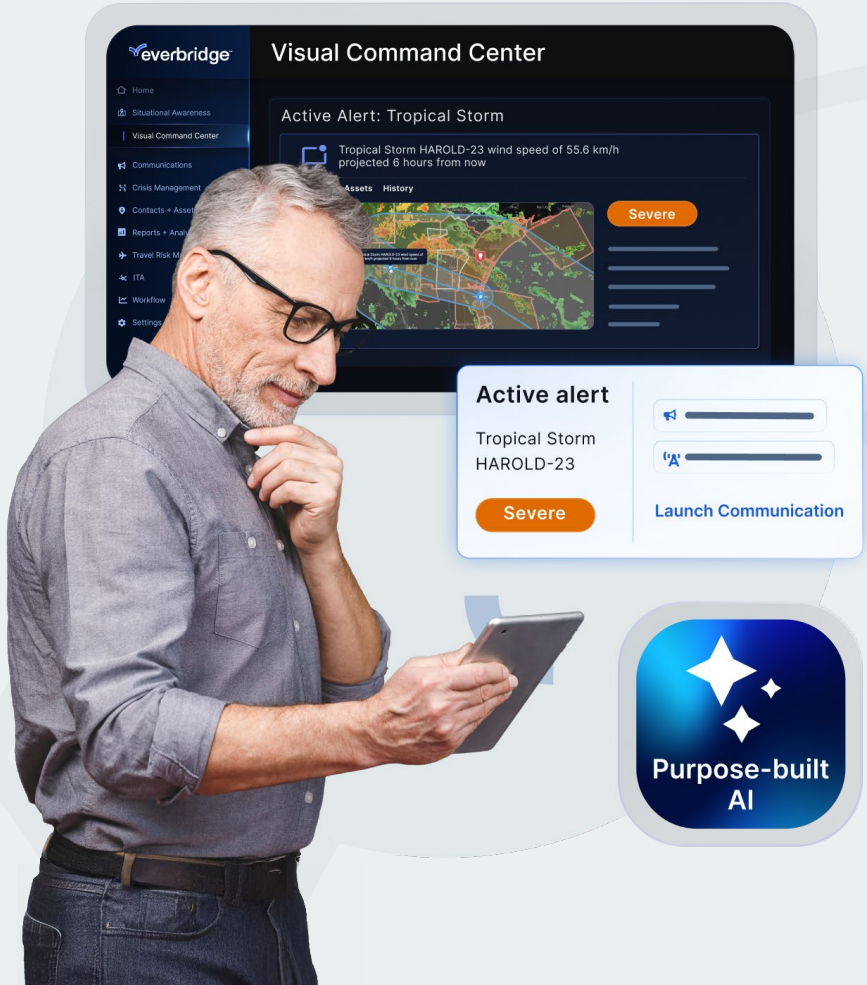
The Everbridge critical event management (CEM) platform empowers organizational resilience by enabling you to know earlier, respond faster, and continuously improve how you deal with potential threats.

Powered by Purpose-built AI, it provides powerful risk mitigation capabilities that are easy to use, streamlining the management of critical events on one seamless platform. It enables you to enhance your emergency response, reduce communication delays, and boost both operational efficiency and organizational resilience.

Experience the power of Everbridge for yourself

Ready to transform how you manage critical events and strengthen your organization's resilience? Request your personalized demo to see Everbridge in action today. Call us at +1 (888) 366-4911 to speak with a resilience expert, or schedule a demo at everbridge.com/demo

Schedule a demo



Additional resources

High Velocity CEM webinar series

Gain expert guidance, practical insights, and real-world solutions to tackle both physical and digital threats. Our ongoing webinar series empowers your team to ensure business continuity and resilience in an ever-changing risk landscape.

Register here →

Rapid Resilience videos

Stay informed on critical global events with timely updates and expert analysis from Everbridge specialists. Our Rapid Resilience videos provide actionable strategies aligned with real-world developments, delivered as events unfold.

Watch here →

Thought leadership insights

Explore thought-provoking articles and videos from industry experts. Resilience isn't just about responding to crises - it's about anticipating challenges, adapting to change, and thriving in the face of disruption. Gain insights from leading voices shaping the future of resilient organizations.

View here →

Explore the Everbridge product suite

Discover Everbridge High Velocity CEM, the industry's most advanced critical event management platform. Combining automation, risk intelligence, and Purpose-built AI, it delivers resilience at scale. Explore our full product suite designed to support your organization in every step of its resilience journey.

Learn more here →

Take a virtual tour

See how Everbridge can transform your organization with a personalized demo tailored to your needs. Select your areas of interest, and we'll deliver a custom video showcasing the solutions that matter most to you.

Visit here →

Online resource hub

Access a wealth of knowledge, including whitepapers, analyst reports, online training, and in-person events. Our comprehensive resource hub equips you with the tools to navigate crisis management, ensure business continuity, and manage today's expanding risk environment effectively.

Explore here →

Next steps

Turn insight into action

The risks outlined in this report demand more than awareness: they require the ability to act decisively. Everbridge helps organizations operationalize risk intelligence, strengthen preparedness, and respond with confidence as threats emerge.

Protect your people, assets, and operations by transforming regional threat insights into proactive, measurable strategies, powered by Everbridge.

Speak with a Risk Intelligence expert

Discuss your organization's specific risk landscape with our specialists. Learn how Everbridge Risk Intelligence helps you identify vulnerabilities earlier, anticipate escalation, and make informed decisions before incidents disrupt operations.

Talk to an expert today →

See High Velocity CEM in action

Experience how Everbridge High Velocity Critical Event Management unifies intelligence, automation, and response in a single platform. See how you can detect threats sooner, respond faster, and continuously improve resilience across your organization.

Schedule a personalized demo →

Disclaimer

About Everbridge

Everbridge is the global leader in Critical Event Management (CEM), helping organizations achieve a true business resilience advantage. With Everbridge High Velocity CEM™, our customers accelerate response times, minimize disruption, and maintain operational control amid today's most complex threats. Using Purpose-built AI, decision-ready risk intelligence, and full lifecycle automation, Everbridge enables organizations to know earlier, respond faster, and improve continuously with confidence.

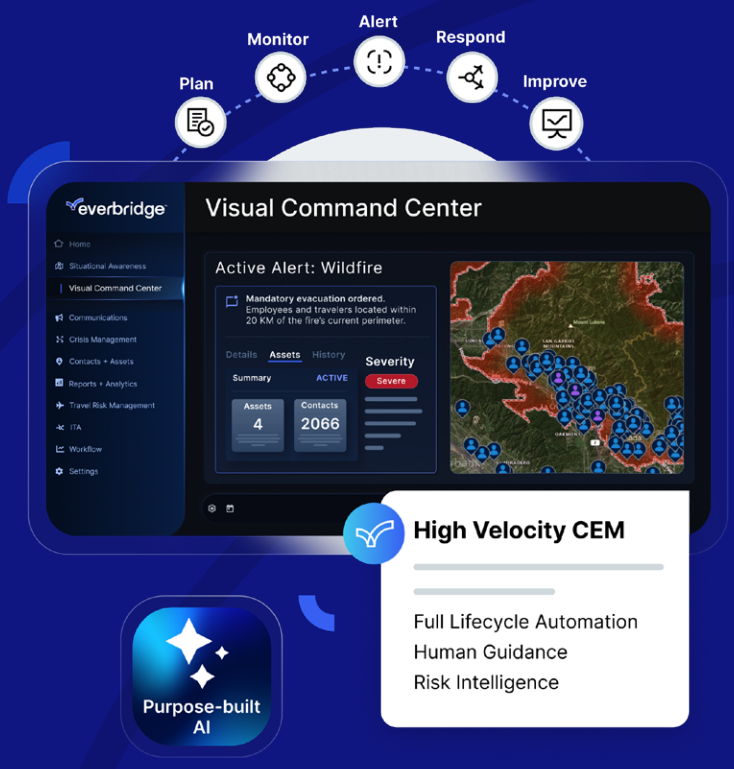
Everbridge... Keeping People Safe and Organizations Running™

Visit Everbridge.com

Read our company blog

Follow us on LinkedIn

Follow us on X



Everbridge delivers a business resilience advantage with High Velocity CEM™, powered by Purpose-built AI and decision-ready intelligence to accelerate response, reduce downtime, and protect what matters most.
Request a demo at everbridge.com/demo or call +1 (888) 366-4911.

WP-EN-2026 Regional threat assessment report _12.22.25