Gradient Cyber Launches Quorum AI

AI-driven detection, analysis, and response that materially reduces security noise and response time for the mid-market

SOUTHLAKE, TX, UNITED STATES, January 20, 2026 /EINPresswire.com/ -- Gradient Cyber, a leading provider of Managed Extended Detection and Response (MXDR) for mid-market organizations, today announced the launch of Quorum AI™ (QAI), a major evolution of its MXDR platform designed to dramatically improve threat detection, analysis, and response through applied artificial intelligence.

> Quorum AI is a mid-market shift. Rather than treating AI as a bolt-on, it's woven throughout the platform - reducing noise, surfacing what matters, and helping customers act with speed and confidence."
>
> *James Hamilton, CEO of Gradient Cyber*

Quorum AI builds on Gradient Cyber's proven network-first analytics and human-led SOC operations, introducing a new AI-driven architecture that enhances how security events are ingested, enriched, correlated, prioritized, and acted upon. The result is faster detection, clearer analysis, and more consistent response across endpoint, network, cloud, SaaS, and identity data sources, without increasing operational complexity for customers.

"Quorum AI represents a fundamental shift in how we scale security outcomes for the mid-market," said James Hamilton, CEO of Gradient Cyber. "Rather than treating AI as a bolt-on, we've woven it into the entire fabric of the platform - from telemetry processing and analytics to investigation workflows and reporting. The goal is simple: reduce noise, surface what actually matters, and help our SOC and customers act faster and with more confidence."

From Data Volume to Decision Clarity

Mid-market security teams face a growing imbalance between the volume of security telemetry they generate and their ability to analyze and respond to it effectively. Quorum AI directly addresses this challenge by applying AI across the full security lifecycle - not just at alert generation.

At the core of QAI is an AI-assisted event processing pipeline that continuously ingests and normalizes telemetry from diverse security and IT systems. Events are enriched with asset context, user identity, threat intelligence, and behavioral signals, enabling more accurate

correlation and prioritization. New AI-assisted analytics help better distinguish early indicators of compromise from routine activity, enabling the SOC to focus attention where risk is highest.

This approach significantly reduces alert fatigue while improving mean time to detect (MTTD) and mean time to respond (MTTR), two of the most critical metrics for effective security operations.

AI-Assisted Analysis and SitRep Generation

One of the most visible advancements in Quorum AI is its impact on investigation and reporting workflows. QAI introduces agentic AI analysis, case management and SOAR capabilities that help synthesize complex, multi-signal incidents into clear, actionable narratives.

Gradient Cyber's industry-leading Situation Reports (SitReps) now benefit from AI-driven context aggregation and drafting assistance, enabling faster delivery of high-quality incident summaries that explain what happened, why it matters, and what actions are recommended. Human analysts remain firmly in the loop, validating findings and recommendations, but with dramatically reduced manual effort.

"For customers, this means even sharper and more tailored SitReps for response and remediation actions," Hamilton added. "For our SOC, it means we can scale expertise without sacrificing rigor or clarity."

Operational Intelligence Beyond Alerts

Quorum AI extends beyond detection and response into broader operational and security intelligence. New dashboards and analytics provide visibility into detection coverage, response effectiveness, automation performance, and risk trends over time. These insights help organizations understand not just individual incidents, but how their overall security posture is evolving.

By linking technical telemetry with business and risk context, QAI enables security leaders to communicate more effectively with executives and stakeholders, bridging the gap between operational security data and strategic decision-making.

Designed for the Realities of the Mid-Market

Unlike platforms built for large enterprises with extensive internal security teams, Quorum AI is designed specifically for the operational realities of mid-market organizations. It integrates seamlessly with existing security tools, avoids excessive tuning requirements, and is delivered as part of Gradient Cyber's fully managed MXDR service.

The platform also supports deployment scenarios that require local processing and resilience,

including environments with limited connectivity, through Gradient Cyber's evolving Quorum Collector architecture.

Availability

Quorum AI will be available in February for both existing and new customers.
Learn more about Quorum AI here.

About Gradient Cyber
Gradient Cyber is a Managed Extended Detection and Response (MXDR) provider purpose-built for the U.S. mid-market. The company combines its proprietary Quorum AI platform with a 24x7 human-led SOC to deliver threat detection, analysis, and response across network, endpoint, cloud, SaaS, and identity environments. Gradient Cyber is known for its network-first analytics, vendor-agnostic data ingestion, and highly contextual Situation Reports that enable faster, clearer decision-making. The company is headquartered in Southlake, Texas.

Neal Hartsell
Gradient Cyber
nhartsell@gradientcyber.com
Visit us on social media:
LinkedIn
YouTube
