MARK43

Mark43 Cybersecurity and Compliance Solutions

Cybersecurity continues to increase as a threat to public safety operations. In a recent survey, 87% of law enforcement agencies acknowledged that their organization experienced a cybersecurity issue in the last year, and there were over 1000 cyberattacks on public safety agencies in the past 24 months costing over $2.5 billion across government agencies. Additionally, achieving and maintaining CJIS compliance increases the complexity for teams responsible for data security at these agencies. In October 2024, CJIS policy changes included over 700 new requirements, leaving law enforcement agencies with the challenge of training and balancing requirements with ease of use.

Further compounding the problem is the shortage of cybersecurity expertise, both in public safety and across all industries. In 2024 there were 4.8 million unfilled cybersecurity positions worldwide, which was almost 20% higher than the year prior.

Mark43 provides three levels of cybersecurity support for partner agencies.

MARK43 PLATFORM

Our cloud-native platform is secured at the physical layer by AWS, and at the application layer by Mark43. Security vulnerabilities are owned, fixed and patched by Mark43 with no responsibility for agencies to secure and maintain hardware or software to protect against vulnerabilities, or prevent disruptions and outages. The platform also supports single sign-on (SSO) integration to enable centralized access management.

87%

of public safety agencies experienced an outage in 2025, leading to slower response times, risk to officer safety, and community frustration

*Survey conducted by Propeller Insights for Mark43

MARK43 FORTIFIED

Automated protection and alerting of your users and data on Mark43.

- Status and Progress: **Dashboards** show current security and compliance posture and **trends** over time
- Detection: **Real-time monitoring and alerts** inform you instantly of risky behavior and violations
- Prioritization: Sortable event logs **prioritize the most critical** issues to address
- Mitigation: **Investigation workflow** guides team through steps to mitigate issues. Audit trail ensures compliance and accountability
- Prevention: SCIM integration **automates user provisioning** and ensures correct access and privileges

MARK43 CYBERCLARITY

Mark43 also provides security and compliance focused professional services that help agencies improve their overall security and compliance readiness and posture. Mark43 CyberClarity includes the following services:

- **CJIS Compliance Assessment**
  Annual audit reviewing all relevant CJIS requirements specific to the agency and providing report highlighting strengths, weaknesses and prioritized recommendations to help the agency strengthen CJIS controls.

- **External Cybersecurity Threat Risk Assessment**
  Annual cyber health test performed on public-facing digital assets and publicly available information about the agency. All known external assets are reviewed for weaknesses, and a comprehensive report is provided detailing the findings, highlighting potential threats and recommending best practices for remediation.

- **Cyber Incident Readiness Drills**
  Annual instructor-led live cyber incident tabletop exercise designed to prepare and practice responses to cyber-related incidents. Simulations of realistic scenarios such as a coordinated ransomware attack against multiple safety agencies, mimicking real-life consequences such as disrupted emergency response times, will be practiced with key personnel, and will culminate with an after-action report containing best practice recommendations for improving response readiness and procedures.

- **Identity and Access Checkup**
  Identity and Access Management (IAM) review of users, permissions and usage in Mark43 to help ensure the security and integrity of sensitive agency information. Provided annually to align with the CJIS requirement for regular reviews, the checkup includes a review of user accounts, highlighting terminated users who still have active accounts, administrative accounts that may be unnecessary, identifying stale accounts, and assessment of groups and profiles. In addition to the review, the checkup includes assistance for improving IAM practices and processes to reduce risk going forward.

- **Security Awareness and Phishing Resilience Training**
  Annual onsite training for all agency staff educating on risks such as malware, phishing and social engineering and best practices to protect against these threats. The service also includes phishing resilience exercises, providing immediate feedback to users and detailed reports to command staff with tailored recommendations to enhance the agency's security posture.