



TEAMING UP AGAINST NEW THREATS

MULTIMODAL ACCESS CONTROL IS THE ANSWER TO EVOLVING THREATS

Critical infrastructure and organizations face increasing threats as physical breaches and cyberattacks grow more sophisticated and interconnected. Traditional security measures like badges, passwords, and PINs often fall short. Implementing biometrics can play an important role in combatting these attacks

■ By: Mohammed Murad, Chief Revenue Officer, Iris ID
mohammed.murad@irisid.com

Facial recognition is more likely to receive buy-in from decision-makers because it is widely understood and used by many in everyday tech. However, iris biometrics, with 99% accuracy, remain stable over a lifetime and are resistant to issues like wear or tampering (common with physical access credentials), making them invaluable in modern security environments – particularly in locations that require the highest levels of security, like data centers, government programs, and critical infrastructure. For example, the NGI (Next Generation Identification – NGI Iris Service Advanced Biometric Identification in Action — BioSpecs) platform, released in 2020 by the FBI, has been used to amass approximately 2.5 million identities (Iris records) and 15 million identities for other federal government databases. The NGI iris database is used in highly sensitive applications like prisoner transportation or release, probation, parole, court appearances, border control management and to identify known and suspected terrorists, underscoring the accuracy, privacy, and trustworthiness of iris recognition.

Integrating iris recognition and multimodal biometric solutions into modern security strategies allows security teams to improve identity verification and access control across diverse settings such as high-risk facilities, corporate environments, and even during emergencies where restricted access is critical.

Countering Evolving Threats in Cyber-Physical Security

The convergence of cyber and physical threats presents new challenges for security teams, law enforcement, and private organizations. Such incidents can disrupt operations, damage reputations, and even jeopardize public safety.

Outdated access systems, such as fingerprint scanners or card-based credentials, are vulnerable to theft and spoofing techniques. Attackers can exploit these weaknesses to infiltrate critical infrastructure or private facilities. Iris biometrics offer a robust alternative, with unmatched accuracy and resistance to tampering.

Consider a ransomware attack targeting an energy company's operational systems. Such an attack could lock operators out of essential controls while simultaneously exposing physical vulnerabilities. Employing a tamper-proof solution, like multimodal biometric access control, would ensure that

only authorized personnel access critical areas during such an emergency, bolstering both cybersecurity and physical security.

Maximizing Iris Recognition for Secure Operations

Iris recognition technology delivers unparalleled advantages for organizations, critical infrastructure, and law enforcement. Its interoperability with existing security systems, including fingerprint databases and Live Scan tools, enables the use of multi-factor security frameworks that are both efficient and comprehensive. This seamless integration improves workflows, ensuring faster, more accurate identity verification while reducing vulnerabilities. The technology's secure management of biometric data and adherence to privacy regulations such as GDPR ensure sensitive information remains protected, building public trust and demonstrating ethical technology use. For instance, encrypted biometric templates and compliance protocols help organizations align with regulatory requirements while maintaining robust security.

Securing Operations Across Industries

Iris recognition represents a turning point in identity verification across industries. Its speed, accuracy, and reliability make



By embracing multimodal identity solutions such as Iris ID's Face and Iris Fusion technology, security leaders can establish a new standard for accuracy, efficiency, privacy, and trust, delivering the right level of authentication for every interaction

it indispensable for protecting both digital and physical assets. When combined with facial recognition in a multimodal approach, organizations gain the flexibility to balance convenience with the highest levels of identity assurance. Iris ID's Face and Iris Fusion technology leverages the strengths of both biometrics: facial recognition as the most convenient and intuitive method of authentication, and iris recognition as one of the most accurate and stable biometric modalities available. The true potential of this technology lies in its ability to scale across both public and private sectors. In enterprise environments, the Iris ID IrisAccess iA1000 secures data centers, network operations centers, laboratories, pharmaceutical facilities, and executive offices by ensuring that only authorized individuals gain access to critical areas. Energy facilities, manufacturing sites, and other

critical infrastructure operators can deploy fusion biometrics to protect sensitive assets, eliminate credential sharing, and maintain comprehensive audit trails.

Unique User Experience

A key differentiator of the next generation iA1000 is its unique user experience. At the center of the device is an innovative circular LCD interface that displays the user's image in real time, intuitively guiding them into the optimal position for authentication. This visual feedback eliminates guesswork, reduces failed attempts, and makes the process natural and seamless for first time and frequent users alike. The iA1000 extends this protection even further through some of the industry's most advanced Presentation Attack Detection (PAD) capabilities. As artificial intelligence enables increasingly sophisticated attempts to impersonate

legitimate users using photographs, videos, masks, deepfakes, and other spoofing techniques, verifying identity alone is no longer enough. Organizations must also confirm that the biometric presented originates from a real, live person. The iA1000 continuously analyzes facial and iris characteristics to detect and reject presentation attacks before an authentication decision is made. This additional layer of defense helps safeguard an organization's most valuable assets, ensuring that convenience never comes at the expense of security. As threats continue to evolve, traditional access control systems based solely on cards, PINs, and passwords are no longer sufficient. By embracing multimodal identity solutions such as Iris ID's Face and Iris Fusion technology, security leaders can establish a new standard for accuracy, efficiency, privacy, and trust, delivering the right level of authentication for every interaction while ensuring that the right person is in the right place at the right time. In a world where identity is the new perimeter, advanced biometrics, an intelligent user experience, and AI-driven presentation attack detection provide the confidence to protect what matters most. ■