Trends in Protecting Critical Infrastructure: It's Not Just Locks and CCTV Anymore

By James Careless

Whether it's airports, train stations, or energy grids, today's critical infrastructure faces unprecedented threats. Criminals, saboteurs, hostile states, and cyber-physical terrorists are exploiting every weakness, digital and physical alike.

Protecting these vital networks now demands more than locks and cameras. It requires layered, intelligence-driven defenses that combine biometrics, AI, advanced surveillance, and cyber resilience.

What is shaping the next generation of security — from biometric verification at stadiums and airports to hydrogen-leak detection in energy grids — and why the future of critical infrastructure protection lies in integrated, multi-layered strategies.

The Power of Biometric Security

Although there are many forms of advanced access control systems available today, there's no doubt that biometric-based systems are now vital for keeping all forms of critical infrastructure safe. Such systems assess the unique physical characteristics of people seeking access against their recorded identities through facial recognition, fingerprints, and retinal scans, among others.

Vincent Bouatou, IDEMIA

"Securing critical infrastructure has become a top priority for both public and private sectors, particularly as threats grow increasingly complex and persistent," said Vincent Bouatou. He is CTO of IDEMIA Public Security, which has over 40 years of expertise in delivering biometric access, border security, and digital identity systems worldwide. "Biometric technology has progressed significantly in both capability and adoption, becoming essential for protecting high-security environments, from airports and military bases to data centers and power grids," Bouatou told TSI magazine. He noted that modern biometric systems are not only more accurate and resilient but also more user friendly. "They integrate seamlessly with broader security infrastructures, delivering real-time alerts, audit trails, and analytics," said Bouatou. "Critically, they comply with international privacy and data protection regulations, combining strong security with

Greg Parker, Johnson Controls

Dominic Forrest, iProov

Alex Reichard, Genetec

Johnson Controls provides Allegiant Stadium located in Las Vegas, Nevada, with state-of-the-art security and life safety systems including security management with per-event mapping, access control and vehicle security detection. Johnson Controls image.

responsible design, speed, and precision."

"Biometric technology has advanced to provide more secure and seamless identity verification," said Greg Parker. He is vice president of life cycle solutions with Johnson Controls, a global provider of smart building solutions. "For example, Johnson Controls systems can use fingerprints, facial recognition and iris scans to replace traditional keycards and PINs. We used these efforts to provide Allegiant Stadium with state-of-the-art security and life safety systems by integrating equipment and technologies including security management with per-event mapping, access control, video management, vehicle security detection, and fire alarm detection. Integration of the video management system with the Las Vegas Metropolitan Police Department helps Allegiant Stadium identify and manage public safety events through built-in identification, alarming and notification systems that can act on the incident, alert the appropriate city responders to engage, and provide orchestrated evacuations through site-wide paging and integrated digital signage and kiosks."

In the travel sector, the drive towards biometrics is coming from two powerful directions: what travelers are demanding and what airports and governments need to operate effectively.

"People are simply tired of the friction in the travel journey," said Dominic Forrest. He is CTO of iProov, which develops facial verification solutions for secure travel and border entry. This is why travelers like biometric identity solutions, because they are faster and more reliable than paper-based systems. "An IATA survey showed that around 73% of people would rather use their biometrics than a paper document," he said.

On the other hand, organizations like the U.S. Customs and Border Protection (CBP) and the Greater Orlando Aviation Authority are dealing with a massive increase in passenger numbers. "Orlando International Airport MCO, for instance, saw over 800,000 more international arrivals in 2024 alone," said Forrest. "They need a way to increase their throughput without compromising security. "That's where our technology comes in: we give them a tool that is not only faster but more accurate than the human eye. We use high-end computing devices to capture video at around 60 frames per second as a traveler approaches. In those two or three seconds, we have hundreds of images to work with."

Honeywell has also integrated biometric scanning into access control, combining it with mobile credentials, cloud-based video, and AI-assisted monitoring. "The use of biometrics is primarily employed at critical infrastructure locations to verify identities with more accuracy," said Ewa Pigna, Honeywell's CTO of security and access solutions. "Typical access control systems of the past and present rely on plastic credentials, which can be handed to someone not authorized to use them. Biometrics can be used to back up such systems, or serve as standalone access systems in their own right."

This comprehensive perspective is shared by Genetec, which provides unified physical security solutions that include video management, access control, and more. "Utilities are increasingly adopting biometric technology in some of their most critical facilities, including highly regulated control centers, operational technology (OT) and industrial control system (ICS) rooms, and power generation sites," said Alex Reichard, Genetec's key account manager of utilities and data centers. "Regulatory frameworks like the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards place strong emphasis on robust authentication practices in these areas, and biometric solutions, such as fingerprint and facial recognition, play a key role in meeting those requirements. However, adoption of biometrics

People are simply tired of the friction in the travel journey according to Dominic Forrest, CTO of iProov. Travelers like biometric identity solutions, because they are faster and more reliable than paper-based systems.

Simo Pikkarainen, ALCEA

David Meyers, H2scan

Jeff Stanek, Honeywell

beyond these high-security zones has been slower, largely due to environmental complexities and connectivity challenges in remote locations."

"While biometric security has developed quickly in recent years, its use in critical infrastructure is progressing more slowly, shaped by regulations and the need for the complexity of operations," agreed Simo Pikkarainen. He is CTO of ALCEA, a global security solutions provider primarily focused on protecting critical infrastructure. "Biometric data is highly sensitive, and protecting it is fundamental to maintaining trust. That is why we work closely with experts and authorities to ensure that, alongside physical and digital assets, personal information is protected just as carefully."

Biometrics is just part of ALCEA's end-to-end approach to critical infrastructure security. "At the heart of our offering is ALWIN, a comprehensive solution that supports customers across the full spectrum of security needs, from traditional access methods to the most advanced digital technologies," Pikkarainen said. "Within this framework, we integrate CLIQ technology, which combines high-security mechanical cylinders with the intelligence of electronic access control. Alongside CLIQ, the ABLOY BEAT keyless locking line answers the demand for connectivity with mobile-based access and remote opening capabilities. And with the ALCEA GATEWAY, we enable seamless integration of connected devices and security solutions, ensuring operators always have the right tool for each situation."

As well, some threats to critical infrastructure have nothing to do with access control. Consider hydrogen leaks, which can lead to devastating explosions if not detected in time. "H2scan's mission is to provide the highest reliability and accurate sensors for mission critical hydrogen applications such as safety monitoring, grid asset monitoring and chemical process control solutions," said David Meyers, CEO and president of H2scan. "Our hydrogen detection systems detect hydrogen leaks or the buildup of hydrogen, allowing early action to be taken to avoid damage to plant and personnel. Examples of infrastructure that we protect include refineries and petro-chemical complexes, hydrogen gas generation (electrolyzers), hydrogen blending and pipelines, and battery-energy storage system (BESS) installations."

This threat applies to transportation critical infrastructure. The reason: "Our asset monitoring offering detects the onset of faults in power transformers, the most critical of the grid and air and rail transport ground assets," Meyers said. "Transformer faults generally evolve over time (months, possibly longer), and these internal faults (arcing or overheating) are detected by measuring the buildup of hydrogen gas as the transformer oil breaks down. Early detection of faults means they can be repaired or removed from service before they fail, often catastrophically."

Beyond Access Control

It is clear that biometric-based access control is a major force in securing critical infrastructure. But it is only one piece of the overall security puzzle. "When you look at protecting critical infrastructure as a whole, it's all about high security," said Jeff Stanek, Honeywell's president of security and access solutions. "To achieve this, you're going to want multi-layers of protection beyond biometrics. So, for us, it starts with integrated safety and security systems. This is access control integrated to your video, to your audio, and to your perimeter detection. Then you bring in advanced surveillance technologies and perimeter protection/intrusion detection systems. And it's no longer just about physical threats, there're cyber threats and how you address cybersecurity in your offering is important now."

Vincent Bouatou reinforced the importance of Stanek's comprehensive strategy for securing critical infrastructure. "Biometric solutions form the backbone of many modern security strategies, but they are most effective when deployed as part of a layered, multi-technology defense," he said. "To counter broader threats, AI-enhanced surveillance tools such as video analytics, thermal imaging, and motion detection are increasingly deployed to detect unauthorized entry, monitor perimeters, and identify abnormal behavior."

Alex Reichard also agreed, but he expands the notion of comprehensive security beyond biometric solutions. "For example, drone detection radars have become essential to secure airspace around critical sites by identifying and tracking unauthorized aerial devices," he said. "Environmental monitoring tools, such as thermal sensors, can be used to detect intruders based on their heat signatures, and perimeter detection systems, such as LiDAR (Light Detection and Ranging), can help protect large facilities by identifying and tracking any

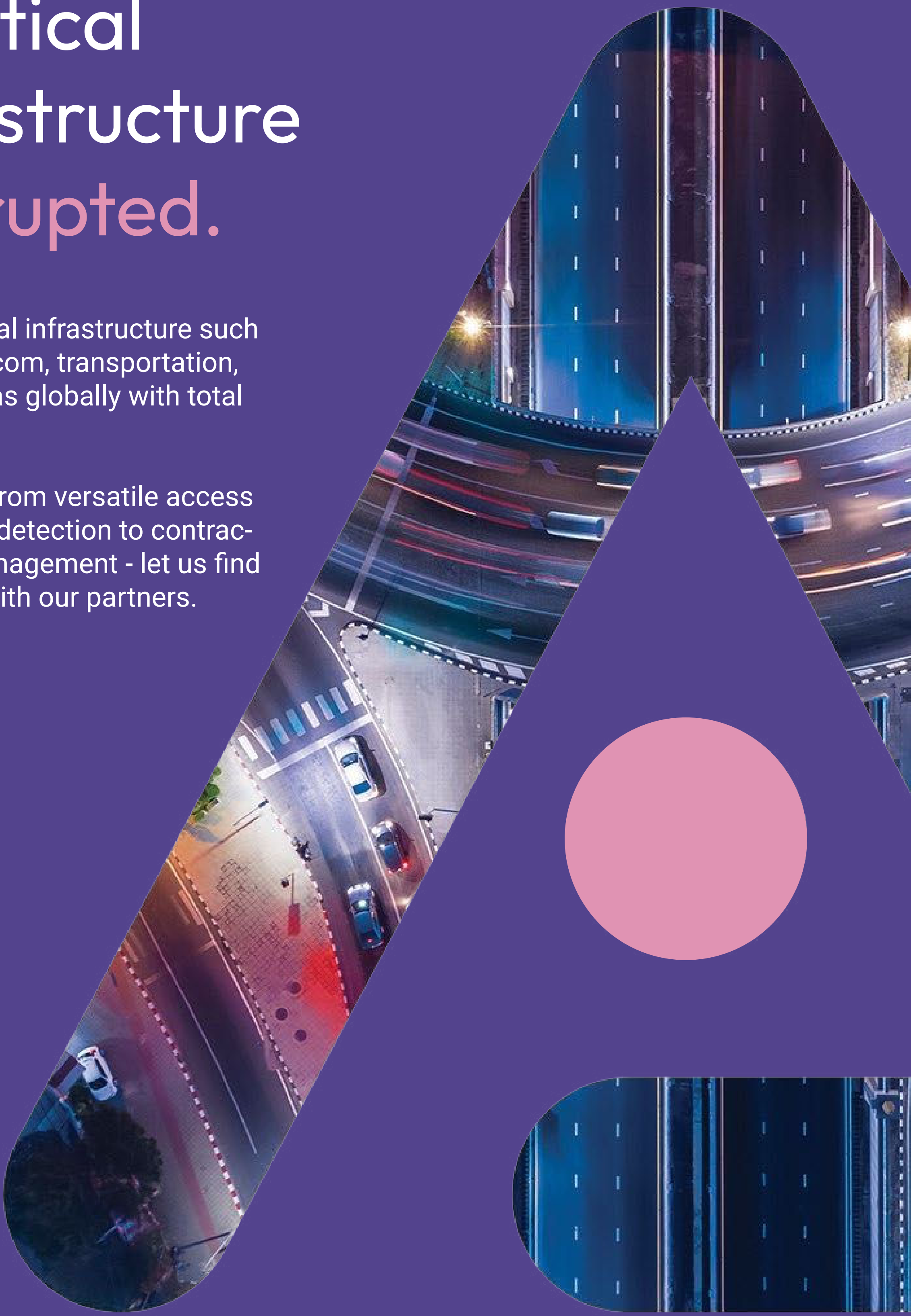
ALCEA

ASSA ABLOY

keep critical infrastructure uninterrupted.

ALCEA protects critical infrastructure such as energy, water, telecom, transportation, mining, and oil and gas globally with total security solutions.

Everything you need from versatile access control and intrusion detection to contractor, key and video management - let us find the solution for you with our partners.



alceaglobal.com

Facilities such as government buildings, utilities, healthcare campuses and other high-priority operations are integrating remote monitoring and lifecycle management into their security systems to maintain resilience and rapidly respond to threats, according to Johnson Control's Greg Parker.

movement beyond the fence line."

Returning to the definition of access control, Reichard noted that card-based systems can be strengthened to improve critical infrastructure security. "For example, technologies like anti-passback systems prevent credential misuse by ensuring that access cards cannot be shared," he said. "Advanced card encryption methods can also be used, such as the Personal Identity Verification (PIV) standard, to enhance physical credential security by preventing cloning and tampering."

Trends That Matter

Several converging trends are affecting the context of critical infrastructure protection. Chief among them are cyber and physical threats, labor shortages, energy pressures, and geopolitical instability.

"The digital transformation of operational environments — especially the convergence of IT and OT systems — has exposed new attack vectors," said Bouatou. "Infrastructure such as transportation networks, energy grids, airports, border checkpoints, and healthcare systems are now targets for sophisticated cyberattacks, often through digital gateways. Geopolitical tensions, state-sponsored threat actors, and organized criminal groups have all increased the risk of targeted attacks on national assets. Real-world incidents, such as power grid disruptions and ransomware targeting hospitals, have underscored the urgency of securing both physical and digital systems."

"Key drivers include the convergence of physical and cyber threats, as the rise of networked building systems requires security strategies that protect both dimensions holistically," Greg Parker noted. "The demand for frictionless, contactless experiences — accelerated in the post-pandemic era — continues to drive the adoption of biometrics and mobile credentials. Additionally, the growing preference for solutions that anticipate vulnerabilities rather than simply react to them fuels the interest in AI-driven insights and managed security services. Reflecting this shift, investment in real-time threat detection has increased by 22%, representing the industry's focus on proactive security measures."

According to Parker, facilities such as government buildings, utilities, healthcare campuses and other high-priority operations are integrating remote monitoring and lifecycle management into their security systems to maintain resilience and rapidly respond to threats. "These solutions aim to mitigate vulnerabilities like physical tampering, insider threats and cybersecurity threats," he said.

In response to the threats above, governments are strengthening regulatory frameworks. A case in point: "The EU's NIS2 Directive and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) guidance are pushing critical infrastructure operators to implement auditable, high-assurance security controls," Bouatou said. "In parallel, zero-trust architecture is gaining momentum. These frameworks require continuous verification of user identity, device integrity, and network behavior — reducing insider threats and limiting lateral movement by attackers."

The widespread adoption of IoT (the Internet of Things), mobile access, AI-driven analytics, and cloud platforms is also expanding the attack surface. At the same time, physical risks including sabotage, natural disasters, and hybrid threats are requiring security systems to detect and address them in real time. According to Bouatou, "these dynamics are accelerating investment in integrated, intelligence-driven security solutions that combine biometrics, AI, big data, and cybersecurity into a unified defense strategy."

Genetec's Reichard added that remote operations and drone incursions represent emerging risks to critical infrastructure. "While remote operations offer flexibility to employees, they require stronger access controls and encrypted communications to keep remote management secure," he said. "We're also dealing with nation-state and geopolitical threats and new risks from the growing use of drones. Put all of that together, and it's clear why there's a growing push for more integrated security solutions that can tackle these challenges."

The human factor also plays a role. At a time when more skilled people are required to manage critical infrastructure security systems, finding qualified employees can be difficult. "Across our industry, there is a shortage of skilled labor," Stanek said. "From what we're hearing from our customers, over 90% of our channel partners are facing challenges in hiring skilled security operators." Fortunately, AI is making it possible to automate many operations that were previously handled by human beings. "It's really about using AI to make security operators more efficient, more intelligent, and more responsive," he said. "That applies not only to critical infrastructure, but really the whole security industry."

In response to evolving challenges, the security industry has developed innovative solutions that enhance protection across multiple areas. "For instance, ID badges now often include built-in certification technology like PIV, which makes them much harder to forge or misuse," said Reichard. "AI-powered video analytics can flag unusual behavior, detect perimeter breaches, or spot unauthorized activity in real time. Meanwhile, on the operations side, managed security services designed specifically for OT and ICS environments provide around-the-clock monitoring and rapid response when something goes wrong. Trend analysis tools also offer valuable insights by analyzing security data over time, allowing organizations to predict and address potential issues before they turn into real problems."

"To meet rising security demands, a new generation of technologies has emerged, designed for adaptability, resilience, and performance," Bouatou added. "For instance, IDEMIA Public Security's MorphoWave can scan four fingerprints in under a second with a simple wave of the hand. It works regardless of finger condition: wet, dry, dirty, or damaged, making it ideal for high-traffic, high-security locations such as airports, stadiums, or research facilities. IDEMIA Public Security's VisionPass and VisionPass SP terminals offer facial recognition with advanced spoof detection and multimodal authentication, using face, card, and PIN. VisionPass SP, in particular, enables 1:1 verification with on-card encrypted templates, ensuring that both the card and the user's face are required for access, making it an effective guard against lost or stolen credentials."

As well, critical infrastructure owners are investing in problem-solving services to secure their properties. This is due to the fact that managed security services allow organizations to outsource complex security functions to experts. Doing so makes advanced security capabilities more accessible and cost-effective to these owners, because such teams can implement 24/7 monitoring, threat detection, and maintenance without their clients having to invest in full-time staff or expensive on-site infrastructure.

"Solutions that provide 360-degree visibility of assets, thereby eliminating blind spots in physical and cyber infrastructures, have become essential to creating peace of mind," said Parker. "AI has also more recently been squarely in the limelight, and we've seen huge leaps in AI innovation and adoption across sectors. In fact, the global AI cybersecurity market was valued at USD $26.55 billion in 2024 and is projected to reach USD $234.64 billion by 2032."

Regarding ALCEA's future plans: "Our connected solutions are expanding into the transport sector," observed Simo Pikkarainen. "These innovations will enhance situational awareness of assets in motion and allow remote control of access, anytime, anywhere. Beyond protecting goods, they safeguard the professionals working within critical infrastructure by enabling remotely controlled access at any time."

"The world of critical infrastructure security is changing rapidly," he concluded. "Connectivity, digitalization, and global uncertainty present new challenges, but also new opportunities." The path ahead is clear: biometric verification, AI-driven analytics and cloud-based monitoring are no longer optional add-ons; they are becoming the backbone of a new, layered defense model. As threats grow more complex, the future belongs to organizations that combine cyber and physical safeguards into unified systems. In short, the winners will be those who treat critical infrastructure not as isolated assets, but as interconnected lifelines — protected by intelligent, adaptive security. TSI

IDEMIA's MorphoWave contactless fingerprint solution scans and verifies four fingerprints in less than one second, through a fully touchless hand wave gesture, the company says. IDEMIA image.