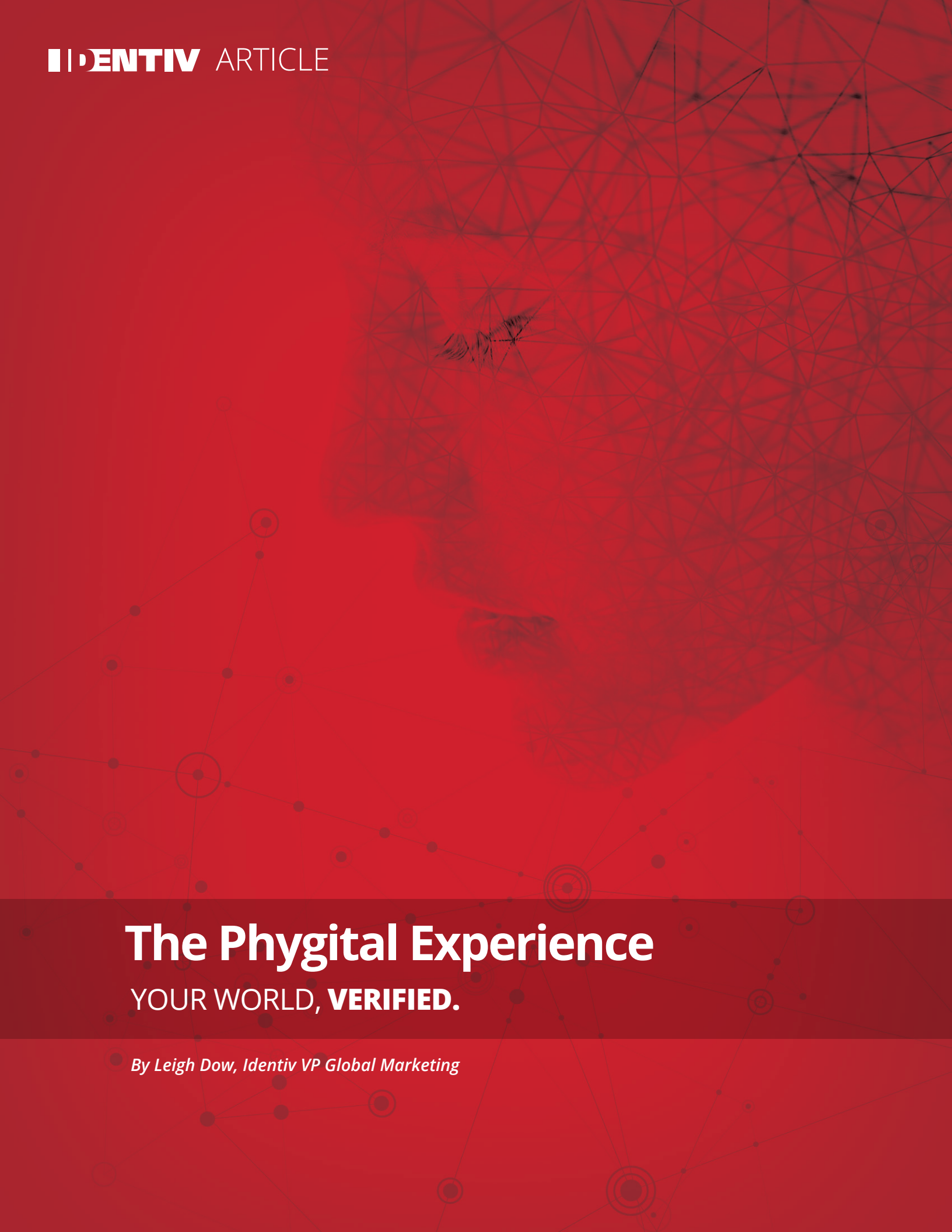
IDENTIV ARTICLE



The Phygital Experience

YOUR WORLD, **VERIFIED.**

By Leigh Dow, Identiv VP Global Marketing

The physical and digital world are interchangeable, making verification the currency to ensure people, products, services, and systems fulfill their intended purpose and have access to the right environment at the right time. When unauthorized users access sensitive information, they steal personal data, plant malicious code, or introduce ransomware. Cyber crime is powerful and impacts places you may not initially consider a cyberattack target. In just the first half of 2021, we witnessed two cyberattacks on critical industries operating heavily in the physical realm: fuel pipelines and meat processing. A "phygital" experience — blending the physical and digital worlds — crosses many of Identiv's core business segments, like physical access control and video, logical access control, credentials, and wireless devices, including radio frequency identification (RFID), near field communication (NFC), and Internet of Things (IoT)-based systems. Regardless of your industry, company size, or phygital environment, Identiv seamlessly integrates with your world, verified.

Verifying Identity with Credentials

From even the earliest implementations of security, a core question stands out: are you who you claim to be? This question persists from old-school and manual verification through cyber and automated security processing. Credentials are available as reusable tokens or as unique, custom identifiers; for example, consider a generic parking pass versus your individual drivers license. These tokens and identifiers may take different forms in physical or digital devices with varying levels of personalization, and are designed to protect physical access and/or information access. However, regardless of their medium, credentials operate in conceptually similar ways.

When examining credentials, we seek out a balance between security processes and user experience. Although employers need confidence their data is protected, employees cannot be overly restricted — innovation is stifled by inefficient security practices. Not only do regular employees require reliable access, there must be a secure, streamlined process to accommodate visitors, temporary workers, and other guests.

The Traditional Physical World

Recent security discussions emphasize cyber challenges, but security was a concern well before the first computer was built. For centuries, we relied on physical devices to restrict access to specific spaces, and we continue to develop these devices. For example, consider how relatively sophisticated even physical locks and keys are today. Beyond a classic lock and key concept, physical credentials take the form of personalized identification, like passports and badges. These may be checked in person, or even by security footage, to monitor multiple physical access points from a single location.

Regardless of industry and application, modern companies require physical protection of personnel, hardware, software, and data. As an everyday example, the Transportation Security Administration (TSA) minds physical security and credentials every time we approach an airport by checking passports and REAL ID. Consumers want to be safe when they fly, but they do not want to wait in hour-long lines. Identiv's expertise with physical access control, video surveillance, and security testing translates this balance between secure access and user experience to any application.

The Growing Digital World

The internet brings unprecedented connectivity, yet also creates unfamiliar challenges in protecting things you cannot touch. Protected digital information can be accessed without any physical contact. However, many of the same big-picture considerations securing the physical world still apply. Users expect a streamlined experience that does not interfere with their ability to quickly find the information or application they need.

There are many aspects to cybersecurity, and one of the most prevalent concerns centers around verifying user identities. In this aspect, we face many identity challenges analogous to the physical world. Just as a physical key can be lost or stolen, so can a password. Passwords have an additional layer of complexity — a weak key might show wear and tear faster, but still remains in the hands of the user. On the other hand, a weak password could allow unauthorized access. A 2017 Data Breach Investigations Report found that 81% of hacking-related breaches leverage either stolen or weak passwords. Digital environments require logical access controls, presenting a new suite of intricate challenges in a rapidly developing cyber threat space. Securing digital information via logical access control requires the expertise of an industry leader, like Identiv, so users can safely and securely access appropriate data.

Becoming Phygital

Identity verification is challenging in any environment, physical or digital. However, traditional credentials may look different in physical environments (for example, a passport) versus digital spaces (a password) — but do they need to be?

For a simple example, consider car keys. While traditionally these were purely physical devices to open doors and turn ignitions, they evolved to include digital components. Not only can you unlock the car, gaining physical access, but you can start the engine and automatically adjust to your saved user settings, adding in logical access. While these two access paradigms – physical access and information access – have traditionally been isolated from each other, the lines between physical and digital security systems are quickly becoming blurred. Taking this process even a step further, car manufacturers are researching biometrics, like fingerprints and facial recognition, to potentially replace physical keys entirely.

As physical locks and keys discover digital counterparts, traditional identification paperwork is evolving in parallel. Drivers licenses are now available on smartphones in many states in the US. Digital vaccine passports are helping expedite border crossings and international travel while protecting sensitive health information. Transforming paper records into readily available mobile and digital apps brings consistency, transparency, and efficiency to overcome bottlenecks in common authentication processes.

The convergence of physical and digital authentication brings a number of benefits, but new security threats are emerging as these applications evolve. These security concerns extend into increasingly complex phygital systems, where conventionally non-digital devices are connected via IoT (or NFC and RFID) to smart systems. Low-profile IoT devices are designed to run simple software on low power with minimal interruption, presenting many challenges when designing security infrastructure. These vast IoT networks of many low power, low storage devices dramatically increase cyber attack surfaces; they commingle roles that were historically designated as either physical security or information security.

Multi-factor authentication (MFA) brings increased security to any verification process. MFA is increasingly common in digital spaces; to log in, a service may require both a password and mobile application acknowledgement. A phygital strategy is even more advantageous, where a physical key turns one lock and a passcode opens the other lock. This two-step security system has proven reliability in both the digital and physical world, and Identiv is leading development to bring in the best of both systems for a phygital experience.

The Cybersecurity and Infrastructure Security Agency (CISA) agrees that systems encompassing both physical and cyber security provide the most comprehensive protection from attacks. As the physical and digital world are becoming more interchangeable, converged phygital security approaches are better prepared to identify, prevent, mitigate, and respond to threats. Convergence encourages information sharing and developing unified security policies across divisions, bolstering overall robustness and resilience.

Looking Ahead

Regardless of environment, language, region, or industry, we will continue to face cyber attacks of ever-increasing sophistication impacting daily life around the world. Access to the right information at the right time is absolutely mission critical: cyber attacks can start fuel and food shortages, steal classified government information, expose personal financial and health information, or cause life-threatening infrastructure failure. From notebooks to tablets, film to files, letters to email, keys to fingerprints — nearly every aspect of our daily life is becoming digital.

While there can be dire consequences when our electronics fail us, there are countless more opportunities for digitization to continue improving lives around the globe. Medical robots have performed delicate, minimally invasive surgeries requiring precision beyond human hands. In emergencies where every second counts, ambulance drones can arrive on the scene far earlier than traditional emergency responders. Self-driving cars hope to reduce the number of injuries and deaths caused by motor vehicles every year. Even with the challenges of a major paradigm shift, our increasingly phygital world continues to transform the human experience in deep, meaningful ways, improving the quality of, and ultimately saving, lives.