FACTSHEET

Convergence of Physical Access Control and Logical Access Control

180 Million Websites

5 Billion Users

50 Billion Devices

Jellyfish not only elevates how you manage current security components, it also enhances future security capabilities. The convergence of physical access control systems with logical access control systems creates a scalable infrastructure which grows with devices, networks and most importantly people.

What is Physical Access Control?

A physical access control system (PACS) is also know as an electronic access control system (EACS). A PACS integrates a variety of hardware (e.g. card-readers, access cards, door locks, turnstiles) and software (access control server, identity database, policy data, control panels) to provide an organization with the ability to control people's access to physical facilities at doorways or other entry ways.[1] A PACS captures data stored in credentials issued to employees and visitors, and the system that creates and provisions them.

A significant proportion of organizations use legacy physical access technologies that are closed systems and have limited ability to integrate with IT infrastructure and limited or no ability to share data with any system outside of themselves. This results in static authentication and authorization mechanisms that burden administrators and end users.

> “As the number of people, devices, services and connections continue to grow by the billions, our systems are no longer only on our physical premises. They are accessed by many devices any time, day or night from anywhere in the world.”

[1] Allan, A & Perkins, E. 2012. *Adaptive Access Control Emerges.* Gartner, Inc.

“Traditionally, physical access control is out of scope with the use of logical access control, Jellyfish changes this.”

What is Logical Access Control?

Logical access control is the use of technologies related to data or information to provide access control to IT systems. Logical access controls are a critical security control, as they set who can access what data, what kinds of access are permitted and denied, why certain users can access data (e.g. correct device, correct user, correct geolocation), and how users can access data (e.g. on a specific device, through a specific application)[2].

To obtain this meaningful data and use it for security purposes, user and entity behaviour analytics (UEBA) tools have to be put in place to observe that behaviours are consistent with what is expected.

Traditionally, physical access control is out of scope with regards to interacting with logical access control solutions. Convergence of physical access control and logical and access control changes this.

What is Convergence?

Organizations have conventionally treated physical and logical security as discrete disciplines. Convergence of physical and logical security allows an organization to achieve better security outcomes.

Cogito Group brings convergence of physical and logical security to life in a new way that strengthens both physical and logical mechanisms. Cogito combines these two common technologies – physical access control and logical access control, then takes it a step further by managing them under a single security platform: Jellyfish.

Cogito’s Jellyfish platform allows for the use of advanced sharing of information even by siloed applications. This allows one system to trigger events in another. Jellyfish’s approach also allows context aware automated decisions to be made that meet the security policy objectives of the organisation. This method assures authentication and authorization methods are used to provide appropriate levels of trust.

Jellyfish provides a consistent, formal environment for context aware decisions. This solves a business problem that many effective security leaders have: the burden of needing to consult with multiple business stakeholders and facilities managers to establish a common approach to securing the environment. Jellyfish offers a mature approach which integrates technology and business processes to create a secure infrastructure.

[2] Wheatman, V. 2018. *Use of IAM for Combined Physical and Network Access Cost Savings and Threat Correlation.* Gartner, Inc.

Benefits of Convergence

- **Security Benefits:** Converged security management can more easily identify and address the vulnerability issues to actively plug those gaps in security. Examples are:
    - Logical access can be blocked because a user has not entered through an area where the computer being logged onto resides. This is despite a remote attacker or trusted insider having the correct credentials to logon with.
    - Automated deprovisioning of access on logical access System based on an account being removed or disabled on the physical access control system.
    - access review and user certification is improved which reduces risk of fraud.
    - Automation produces consistent outcomes that meet the security policy of the organisation.
- **Operational Benefits:** Converged security eliminates the time-consuming need to manage multiple systems, reduces need for auditing, reduces user administration cycle time, and improves risk management productivity. For example:
    - Automated provisioning of the physical access credential based on a new entry in the logical access system and vice versa.
    - Setting and updating facility access rights on the physical system based on changes in logical access permissions for an account.
    - Automation produces consistent outcomes with no errors.
- **Financial Benefits:** Consolidation of common technologies yields cost saving in productivity as tasks are automated. Convergence also removes the ongoing costs of multiple systems being actively managed and reduces recovery costs from security incidents.
- **Compliance Benefits:** Converged security systems make reporting simpler, by automatically separating report creation, review and analysis.

Cogito Group is an award-winning ICT company specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies.