Fact Sheet

Cogito Group

Convergence of PACs and LACs

What is Physical Access Control?

Physical Access Control systems (PACs), are also commonly known as Electronic Access Control systems (EACs). PACs integrate 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] PACs capture data stored in credentials issued to employees and visitors, and the system that creates and provisions them.

180 Million Websites

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

5 Billion Users

A significant proportion of organizations use legacy physical access technologies that are closed systems with 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.

50 Billion Devices

Traditionally, physical access control is considered a separate entity to logical access control, but Cogito Group's 'Jellyfish' changes this. '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.

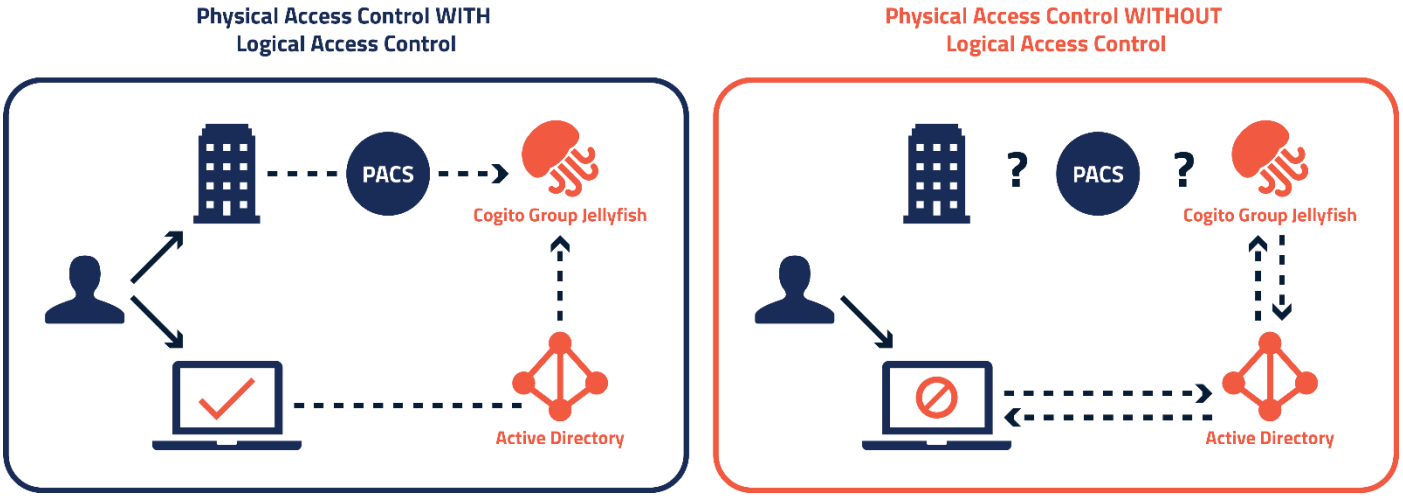
What is Logical Access Control?

Logical Access Control systems (LACs) are technologies related to data or information to provide access control to IT systems. LACs 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].

Convergence of PACs and LACs

Fact Sheet

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. Much like with PACs, Cogito Group's 'Jellyfish' elevates an organisation's LACs security infrastructure.



What is Convergence?

Organizations have conventionally treated PACs and LACs as discrete disciplines. Convergence of PACs and LACs allows an organization to achieve better security outcomes. Cogito Group brings convergence of PACs and LACs to life in a new way that strengthens both Physical and Logical mechanisms. Cogito combines the two disparate security systems, then takes it a step further by managing them under a single security platform: 'Jellyfish'.

Cogito Group'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.

Convergence of PACs and LACs

Fact Sheet

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 LAC system based on an account being removed or disabled on the PAC 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 PACs credentials based on a new entry in the LAC system and vice versa.
- Setting and updating facility access rights on the PAC system based on changes in LACs permissions for an account.
- Automation produces consistent outcomes with no errors.

Financial Benefits

Consolidation of common technologies yields cost savings 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.

Convergence of PACs and LACs

Fact Sheet

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated 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. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.

[1]Allan, A & Perkins, E. 2012. Adaptive Access Control Emerges. Gartner, Inc.
[2]Wheatman, V. 2018. Use of IAM for Combined Physical and Network Access Cost Savings and Threat Correlation. Gartner, Inc.