ARDEXA
Secure by design

What makes Ardexa security so effective?

It is well accepted that effective data and physical asset protection comes from holistic approaches, not just collections of isolated features. Fragmented efforts are unlikely to protect against an increasingly sophisticated cyber threat.

Ardexa has been architected with security at its core, and therefore has the advantage of broad and multi-layered protection against modern cyber threats. Asset managers that have to protect new and legacy assets from these threats must seriously consider such implications in any new system that is introduced, as it is likely to be used for many years to come. Here are some of the principles that make Ardexa so effective.

Do not open plant or machine networks to the Internet

Ardexa connections do not require the external firewall of a network to be opened in any manner. Therefore the plant or machine cannot be accessed through open ports. There are no services open to the Internet or the local network. Ardexa achieves this by the use of a local device at a plant, managed by a sophisticated agent that can connect and protect legacy machines and networks that may not have strong cyber security capabilities. There is no need for public IP addresses, VPN or similar legacy methods.

Treat every command as a message to enable security monitoring

Using Ardexa's message-based infrastructure, one can audit and monitor the system far more easily. There are no VPN tunnels or hidden exchanges that can shelter unauthorised or unwanted actions. Also, if required, individual messages can be authenticated at very fine levels, which is something that will be required in modern multi-actor data exchanges.

Use digital certificates to identify, authenticate and encrypt

Identification and authentication may seem simple, but can suddenly become very difficult when dealing with machines (not humans). This is compounded with high volume, dispersed and remote machines. By using digital certificates, Ardexa can identify machines without the issues that affect passwords. Furthermore, Ardexa uses the digital certificate to simultaneously encrypt and authenticate. These digital certificates are renewed as per the client security policy for added protection, and can be revoked or isolated, if risk mitigation is required. Our API and Web App utilise modern and trusted TLS standards and multi-factor authentication is also available for high-risk environments, as an additional layer of protection.

Protect "weaker" legacy systems behind "stronger" gateways

Most IoT implementations around the world need to connect legacy machines and networks, many of which have poor cyber protection. Many legacy systems have industrial communication protocols with little or no security capabilities. To this end, it is often important to shield these "weaker links" behind robust devices. Ardexa can provide such protection with high quality firewalled devices at each plant, tightly controlled by advanced agents.

Log all actions and data to learn behaviour and improve protection

By logging all commands and actions, Ardexa has the capability to monitor system use and possible intrusions. Data is stored locally and in the cloud, ensuring against data loss due to device or Internet disruptions. Importantly, recording history forms the foundation for future machine learning and security automation.

Maintain remote software as new threats and innovations appear

Remote software that cannot be regularly patched is a potential security risk. Ardexa ensures that all cloud and remote software systems can be updated automatically or manually, at any time. Our agents and plugins in remote locations are regularly updated with new performance and security features, keeping up with releases in connected machines and security policy changes.