ARDEXA
Secure by design

Why Ardexa cybersecurity leads the industry

Our key principles for all industry sectors

Do not open plant or machine networks to the Internet

Use digital certificates to identify, authenticate and encrypt

Shield “weaker” legacy systems behind “stronger” gateways

Authenticate user access rigorously with tightly defined limits

Integrate secure remote working methods seamlessly

Maintain software remotely as vulnerabilities are identified

Inspect every command to detect unwanted actions

Audit all actions to ensure compliance

ARDEXA
Secure by design

Ardexa has been architected with cybersecurity at its core, enabling the advantage of broad and multi-layered protection against modern cyber threats. Organisations must seriously consider cybersecurity implications, especially when it relates to critical infrastructure and/or the security of systems operated by a client organisation.

Do not open plant or machine networks to the Internet

Ardexa connections do not require open ports or external network firewalls to be opened to incoming connections. There are no services open to the Internet or the local network. Ardexa achieves this by the use of a local edge device at a plant, managed by a the Ardexa agent that can connect and protect legacy machines and networks that may not have strong cybersecurity capabilities. There is no need for public IP addresses, open ports or other legacy methods.

Use digital certificates to identify, authenticate and encrypt

Identification and authentication is highly complex when dealing with many dispersed and remote machines (not humans). Using digital certificates, Ardexa can simultaneously identify, encrypt and authenticate individual machines without the issues that affect passwords. These digital certificates are unique to each edge device, renewed 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.

Shield “weaker” legacy systems behind “stronger” gateways

Most organisations need to connect legacy machines and networks, many of which have industrial communication protocols with little or no security capabilities. It is important to shield these “weaker links” behind robust devices. Ardexa can provide such protection with high security devices at each plant, tightly controlled by advanced agents.

Authenticate user access rigorously with tightly defined limits

When dealing with dispersed portfolios, access must be only granted to authorised personnel. Ardexa has a comprehensive permissions set, from entire portfolio control, to read-only monitoring on a single device. Complementary to access control, multi-factor authentication is available and strongly recommended.

Integrate intelligent remote working methods seamlessly

Legacy remote access methods for maintenance, repairs, and diagnostics used by authorised personnel or third-party vendors can create unintended cybersecurity vulnerabilities at your plants. Ardexa uses tunnels and VPNs (highly secure access gateways) that allow access to a single machine or a network, while greatly reducing the risk of malware. All tunnel and VPN access is via Ardexa products, which are all audited and controlled by cloud-based permissions.

Maintain software remotely as vulnerabilities are identified

Software that cannot be regularly patched can lead to serious cybersecurity risks. Ardexa ensures that all cloud and software systems can be remotely updated automatically or manually, at any time. Our devices are regularly updated with new performance and security features, keeping assets secure while minimising downtime.

Inspect every command to detect unwanted actions

Using Ardexa's message-based infrastructure, one can audit and monitor the system far more easily. There are no hidden exchanges that can shelter unauthorised or unwanted actions. Individual messages can be authenticated at very fine levels, a feature that many modern multi-actor data exchanges require. Additionally, Ardexa enables rapid and vital scanning of entire portfolios to identify any active or dormant threats that may be present but unknown.

Audit all actions to ensure compliance

Ardexa logs all commands and actions to monitor system use and provide a sounds basis for security compliance. Audit data is stored in the cloud as an immutable data store, unable to be deleted. All actions relating to the use of the cloud, commands or file transfers to edge device, use of remote working tools are all logged to the cloud.