# Was macht Ardexa IoT so sicher und effizient

„Security at its Core“ – von Beginn an wurde in jeder Entwicklungsphase höchster Wert auf die sichere Gestaltung und Architektur unsere Software gelegt. Dieser Grundsatz ermöglicht es uns einen umfangreichen Schutz, auf mehreren Ebenen, gegen jegliche moderne Cyber-Bedrohung anbieten zu können. Ob moderne oder alte Anlage, jeder Betreiber sollte sich der Auswirkungen eines unzureichenden Schutzes bewusst sein. Hier einige Beispiele, warum Ardexa IoT als so sicher gilt.

**Kein direkter Zugriff aus dem Internet auf Maschinen- oder Anlagen-Netzwerke**

Das Ardexa System nutzt und fordert keine Lücken in bestehenden Firewalls, dadurch kann auch kein externer Zugriff über offene Ports erfolgen. Es gibt keine Dienste, welche mit dem Internet oder dem lokalen Netzwerk verbunden sind! Erreicht wird das durch ein Agent-Broker-Konzept. Vor Ort an der Anlage ist nur ein Standard Gateway notwendig. Auf diesem Gateway läuft ein nach allen Anforderungen der modernen Cyber-Security ein hochentwickelter Ardexa Agent. Dieser ermöglicht einen absolut sicheren Zugriff auf Ihre Anlage, auch wenn diese selbst über keinerlei Sicherheits-Features verfügt.

**No VPN - jedes Kommando ist eine Nachricht, für ein sicheres und lückenloses Monitoring**

Durch unser Nachrichtenbasierte Infrastruktur wird jedes Command zu einer Nachricht, es wird geloggt und kann somit lückenlos überprüft werden. Audits werden viel einfacher. Es werden weder VPN-Tunnel noch andere Lösungen mit verstecktem Datenaustausch genutzt. Hinter welchen sich oft unautorisierte oder ungewollte Zugriffe verstecken können. Es können auch, sofern benötigt, einzelne Nachrichten authentifiziert werden. Dies ist besonders wichtig, wenn der Datenaustausch zwischen mehreren Unternehmen und/oder Dienstleistern erfolgt.

**Digitale Zertifikate zur Identifizierung, Authentifizierung und Verschlüsselung**

Identifizierungen und Authentifizierungen von Menschen ist ein Einfaches, jedoch stellt die Identifizierung und Authentifizierung von Maschinen viele vor eine große Herausforderung. Die oftmals weit verstreuten und schwer zugänglichen Anlagen machen diese Herausforderung, neben der oftmals großen Anzahl von Anlagen, zu einem Kernproblem.

Mithilfe von digitalen Zertifikaten werden Maschinen mit Ardexa identifiziert. Weiter nutzt Ardexa diese digitale Zertifizierung für eine umfangreiche Authentifizierung und Verschlüsselung. Diese digitalen Zertifikate werden entsprechend den Kundensicherheits-Richtlinien erneuert und können jederzeit widerrufen oder extern verwaltet werden, um das Risiko weiter zu reduzieren. Unsere API und Web-Applikation nutzt modernste, vertrauenswürdige TLS-Standards, Multi-Faktor Authentifizierungen bieten für Anlagen mit hohem Risiko einen zusätzlichen Schutz.

**Schutz von „schwachen“, veralteten Systemen mithilfe von modernen Gateways**

Die meisten IoT-Anbindungen erfolgen an veralteten Systemen, welche viele unterschiedliche industrielle Datenprotokolle mit mehr oder weniger sicheren Sicherheitsfunktionen nutzen. Diese Schwachstellen werden von Ardexa mithilfe von hochentwickelten Firewalls und Agenten geschützt.

**Protokollieren Sie jede Aktion, um Verhaltensmuster zu erkennen und die Sicherheit zu verbessern**

Dadurch, dass alle Kommandos und Aktionen protokolliert werden, bietet Ardexa die Möglichkeit jegliche Nutzungsaktivitäten und Eindringversuche in das System aufzuzeichnen. Alle Daten werden lokal am Edge-Gerät und in der Cloud gespeichert, um einem möglichen Verlust durch Hardware- oder Internet-Probleme vorzubeugen. Die Aufzeichnung aller Aktivitäten ist die Grundlage für maschinelles Lernen und die Automatisierung der Sicherheit.

**Software warten und an neue Gegebenheiten und Gefahren anpassen**

Jede Remote-Software, welche nicht regulär gewartet wird, ist ein potenzielles Sicherheitsrisiko. Ardexa stellt sicher, dass jedes unserer Cloud- und Remote- Systeme automatisch oder manuell zu jeder Zeit gewartet werden kann. Unsere Remote Agents und Plugins werden regelmäßig mit neuesten Performance- und Security-Features aktualisiert, ohne den laufenden Betrieb zu gefährden.