ECOPLANT

SECURITY OVERVIEW

CONTROLS ARE AN ESSENTIAL ELEMENT OF DATA SECURITY.
HERE ARE SOME OF THE ONES THAT ECOPLANT HAS PUT IN PLACE TO PROTECT YOUR INFORMATION:

DATA TRANSMISSION AND STORAGE

- Securing data transmission and data is a top priority for Ecoplant for both in-transit data or inactive/at-rest data.
- Ecoplant's solutions leverages the AWS (Amazon Web Services) cloud platform. Built with security from the ground up, these systems take advantage of AWS's robust protected environments, including data encryption.

DATA BACKUP AND DISASTER RECOVERY CONTROLS

- Ecoplant ensures that backups for all critical systems are tested and maintained, and that backup media is secured and available for use in an emergency. Ecoplant's management reviews these controls and ensure compliance annually.

ECOBOX (EDGE)

- Private APN
- EcoBox driven session
- EcoBox local engine operation
- Authentication based local access
- Corporate Network Option - IP restrictions, firewalls, DMZ
- Tamper alert (optional)
- Periodic Security Patch update
- Annual EcoBox Vulnerability testing

IoT COLLECTION SERVICE

- Bi-directional MQTT over TLS/TCP (port 8883 or 443)
- EcoBox are authenticated using X.509 Certificate

CLOUD INFRASTRUCTURE

- VPC security, Access control list
- Data in-transit encryption (ECDHE-ECDSA-AES128-GCM-SHA256)
- Data at-rest encryption (KMS)
- Cloud security monitoring services
- Annual Web-app Vulnerability testing

AUTHENTICATION

- SSO (AWS Cognito)
- Password strength
- MFA
- LDAP Integration (Roadmap)

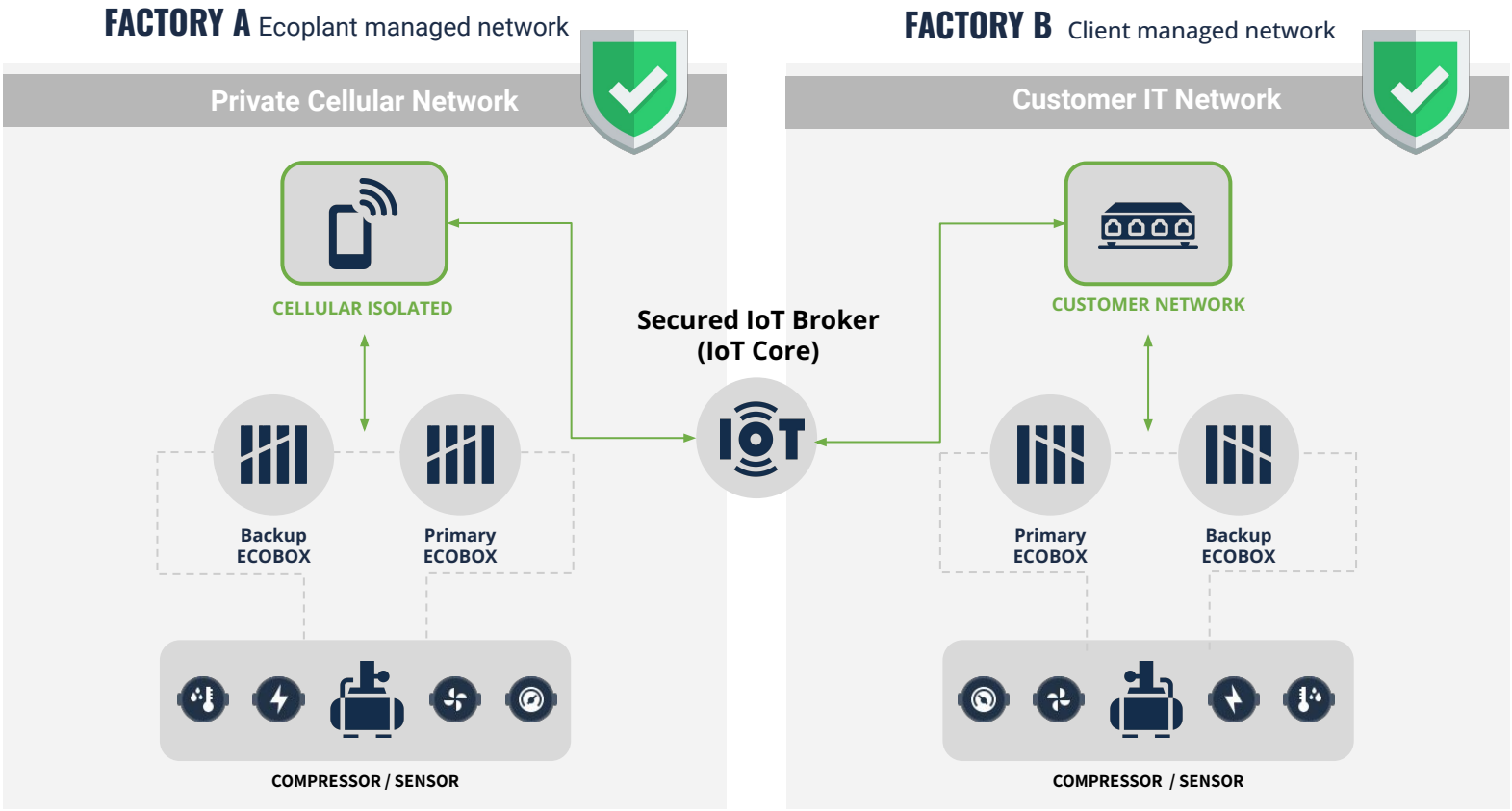
DATABASE

- VPC only access
- Customer data separation
- Role based authentication

SECURED R&D

- Private Github code repository and development environments
- OSS security alerts monitoring (Snyk)
- Secured coding guideline and review process
- Periodic Policy review and Training

NETWORK ARCHITECTURE OPTIONS
ECOPLANT 360



- Ecolab/Ecoplant provide our customer a flexible design to be meet their IT / Security guidelines

- **Option 2 (Factory B)** - Will work closely with our customer to best implement according to their policies and design controls

- **Option 1 (Factory A)** - Private cellular network, not to connect to existing customer IT network. Quicker deployment

ADDITIONAL INFORMATION

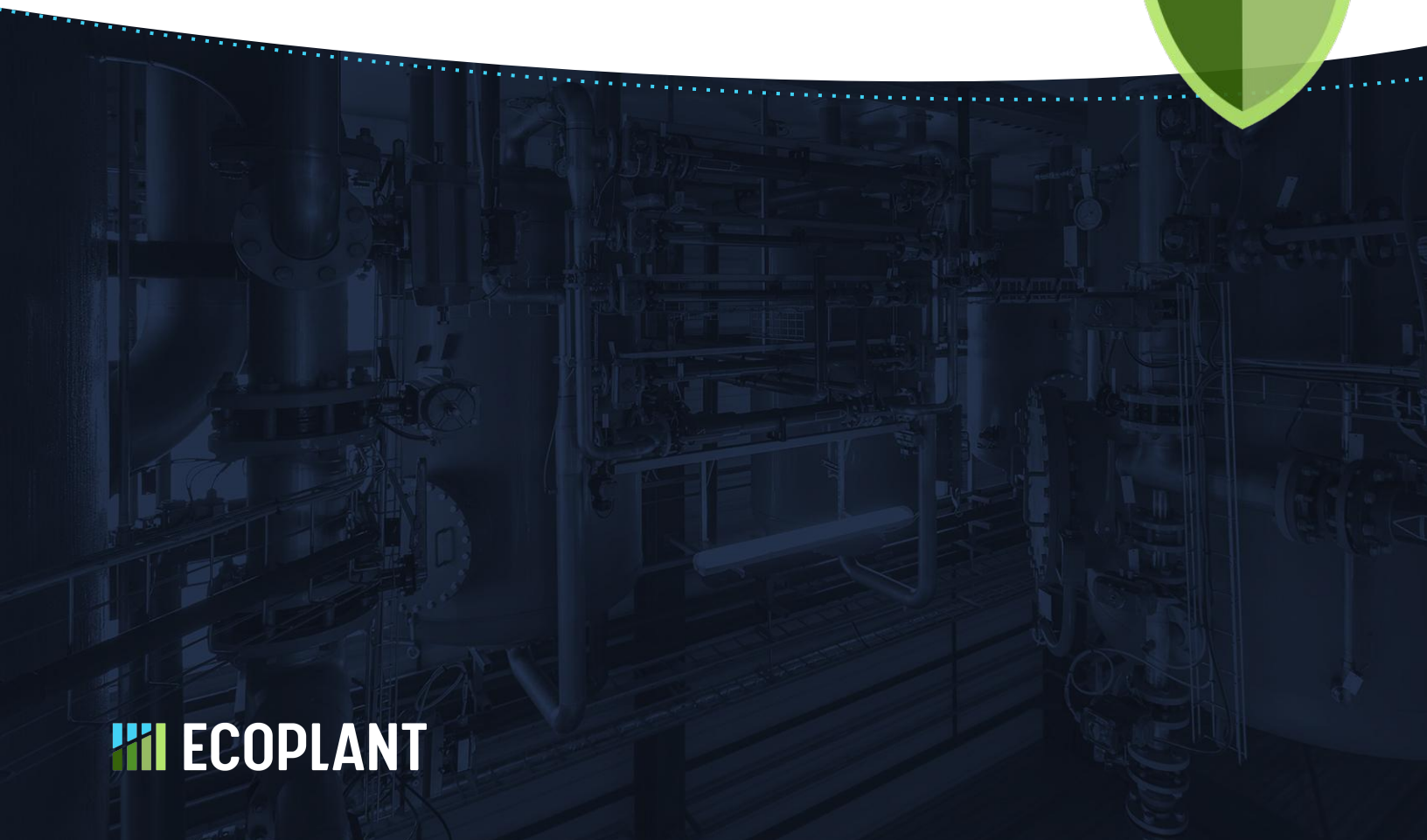
- No one document can answer every question about data security. If you would like more information about Ecoplant's systems and how we protect your information, we are happy to speak with your staff or IT personnel. Your account representative can facilitate that discussion with our team or you can submit a request at info@ecoplant.co arrangements to provide you with the answers that you need.

RISK MANAGEMENT AND AUDITS

- Ecoplant develops and periodically reviews formal, documented information security policies, including risk management. Other policies include: security awareness, security training, incident response, and identity and access management. Formal, documented procedures facilitate the implementation of Ecoplant's policies and associated risk assessment controls.
- Ecoplant conducts periodic penetration testing and security program reviews.

ADDITIONAL INFORMATION

- No one document can answer every question about data security. If you would like more information about Ecoplant's systems and how we protect your information, we are happy to speak with your staff or IT personnel. Your account representative can facilitate that discussion with our team or you can submit a request at info@ecoplant.co arrangements to provide you with the answers that you need.



ECOPLANT