

AirC Connect Cyber Security

AirC Connect is a service developed by Munters that enables secure remote climate control through a cloud solution. By connecting the dehumidifier with a gateway, users can log in and access personalized features via an intuitive web interface. Munters has implemented robust security measures, processes, and guardrails to ensure the safety of infrastructure, data storage, and software design, detailed below.

Authentication

- **Single Sign-On (SSO):** Munters uses OAuth 2.0 with multi-factor authentication and short session timeouts to safeguard customer data.
- **Access segmentation:** Environments and resources are segmented with Role-Based Access Control (RBAC), including machine-to-machine API access.

Encryption

- **End-to-end encryption:** All traffic, both internal and external, is encrypted with TLS 1.2 and 1.3. The identity of both the client and server is mutually verified.
- **Database encryption:** Databases are encrypted with AES-256 using secured using RSA-256 service-managed and customer-managed keys.

Network Security

- **Traffic monitoring:** Internal and external network traffic is monitored, analyzed, and inspected using tools such as Rapid7 and Microsoft Sentinel.
- **Security integration:** Application and internal protection are integrated with a Security Event and Incident Management (SEIM) platform.

Security principles

- **Continuous evaluation:** AirC services, infrastructure, and software undergo continuous evaluation against various security frameworks, including:
 - NISTIR 8259
 - NIST SP 800-57, SP 800-131, SP 800-38
 - ETSI EN 303 645
 - ENISA Guidelines for Securing IoT
 - Microsoft Azure cloud best practices

Regulatory compliance

Munters' AirC Connect complies with several key cybersecurity regulations, including:

- EU Cyber Resilience Act (2019/1020)
- EU NIS 2 Directive (2022/2555)
- EU Data Act (2023/2854)
- EU GDPR (2016/679)
- US IoT Cybersecurity Improvement Act of 2020
- California IoT Security Law (SB-327)
- Oregon IoT Law (House Bill 2395)

As the service expands into new markets, Munters will ensure compliance with additional regional cybersecurity regulations.