Waterly Cybersecurity FAQs

Detailed IT FAQs regarding Waterly and WaterClick Partner EWON (Flexy 205)

1. **Is Waterly data encrypted in transit?**

   Yes, all data is encrypted in transit between Waterly application components, our partners and our customers.

2. **Is Waterly data encrypted at rest?**

   Yes, Waterly customer and application data is encrypted at rest. Additionally, all employees have mandatory encryption on local devices, so any development data sets are also encrypted.

3. **What is Waterly's backup RPO? What is the RTO?**

   Recovery Point Objective (RPO) and Recovery Time Objective (RTO): Waterly's primary hosting environment is located in Microsoft Azure's East US 2 region, with some small services that are provided by other hosting providers. Our application services utilize Kubernetes, a system that provides application redundancy and self-healing features. Our applications and database systems are redundant, load-balanced and run across multiple availability zones, with sufficient spare capacity in case any set of nodes becomes unavailable. We use standards-based infrastructure automation that allows us to re-create the entire Waterly hosted environment (if it was ever needed) within hours, not days or weeks.

4. **How is data backup handled? Can the system be rolled back in case of data corruption or user negligence?**

   All data in Waterly is configured for continuous backup. Data is restorable to any exact moment within the past 30 days (with millisecond precision). In addition, customers cannot delete data…only mark it as archived. Depending on the data outage/failure, we can fail to another redundant database node or recover a full database in minutes to a new node.

5. **Can an individual customer's data be restored to a point in time without affecting multiple customers?**

   Yes, but we would have to do it manually behind the scenes. If needed (it has not been needed, to date), this would take us hours and not days. Additionally, Waterly maintains full audit logs of every data and configuration change to the system, allowing both customers and Waterly staff to collaboratively "undo" a change if needed.

6. **Can a customer/user backup or export their data? Can that backup/export be automated?**

   Customers can download a month of all of their data at any point without us involved. We do not have a way for a customer to automate a separate backup themselves at this time, but if you want to fill out a support ticket periodically, we'd be happy to ship you a full set of your data.

7. **How are users authenticated? Is two factor auth supported, and if so what types?**

   We have two options: An internal app login/password or an SSO option that can support 2FA.

8. **Can our existing identity infrastructure be used via SAML or other Single Sign On methods?**

   Yes. We can support OIDC flows today out of the box. SAML is on our radar with no specific timeline, but happy to discuss.

9. **Are there dashboards / statistics available regarding both real-time and historical system availability?**

   Yes. We have a live app status dashboard: https://status.waterlyapp.com We've had about a total of 5 hours of unplanned downtime over the past three years. Our (planned) deployments are typically Monday nights and last a few seconds to customers that might be logged into Waterly after 9p Central.

10. **Are any industry standards / certifications adhered to such as SOC2 or FedRAMP?**

    We do not have specific SOC2 or other certifications today. Our team comes from a long history of regulated and certified environments across HIPAA, PCI, SOC2, etc., and have built systems accordingly. From a physical systems perspective, we are hosted within the Azure environment, and thus inherit processes from them on that standpoint. From a process standpoint, we'd be happy to answer any specific questions that you might have.

11. **Does Waterly or your subcontractors have recurring datacenter and application security audits completed?**

    We do have monthly basic, automated scans occurring across the environment, but have not, to date, engaged in a full audit and/or penetration test.

12. **How does the provider control and log access to customer data by their employees and/or any subcontractors?**

    Access is provided on a least-privilege basis. Any updates to customer data is logged under the same provision that customers are logged as well. We log who, when and what was changed, from a data perspective.

13. **Does Waterly or our subcontractors have a secure data destruction policy/process for customer data, equipment not in service and removable media?**

    We do not. If a customer wants to terminate service, we would be happy to destroy the data if they request it. As a practice, customer data does not exist on non-controlled environments. In our operational/cloud environments, data destruction happens as inherited by Azure procedures for safe data handling. We do have data-handling policies in place for employees and contractors that may, as an exception, have customer data on their own machines for reporting or analysis purposes.

14. **How does the provider inform us of a data breach or other security incidents?**

    All customers will be informed of any data breach via email. You'd probably get a call from a member of our team if you had any specific concerns.

15. **Does the vendor or their subcontractors have data security or cyber liability insurance?**

    Yes, Waterly has cyber liability insurance and $2MM of General Liability and Professional Liability.

16. **Where is Waterly's data stored/hosted?**

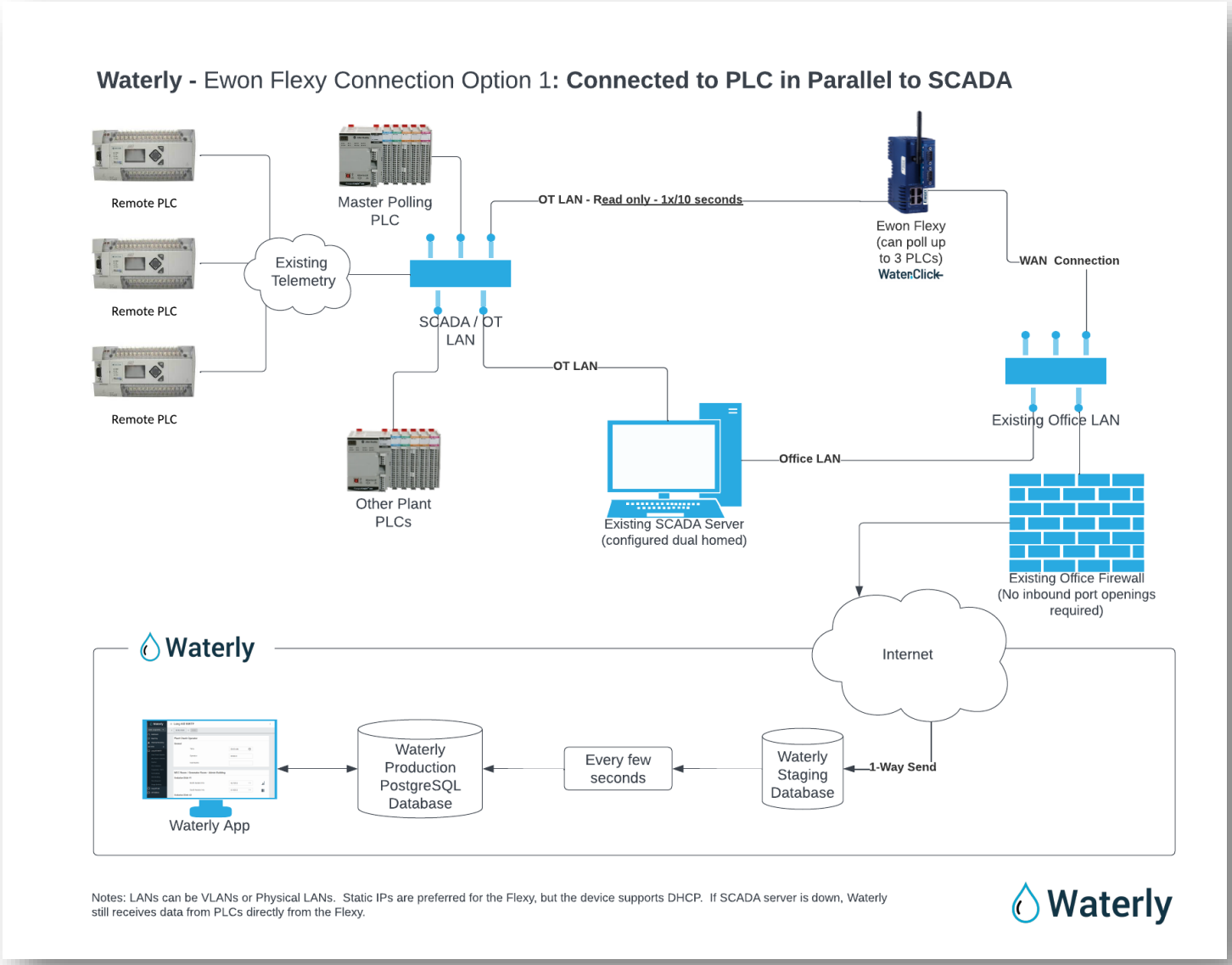
    Waterly's data is stored in the United States, specifically the Microsoft Azure US-based facilities.

17. What are my options for connecting SCADA data to Waterly?

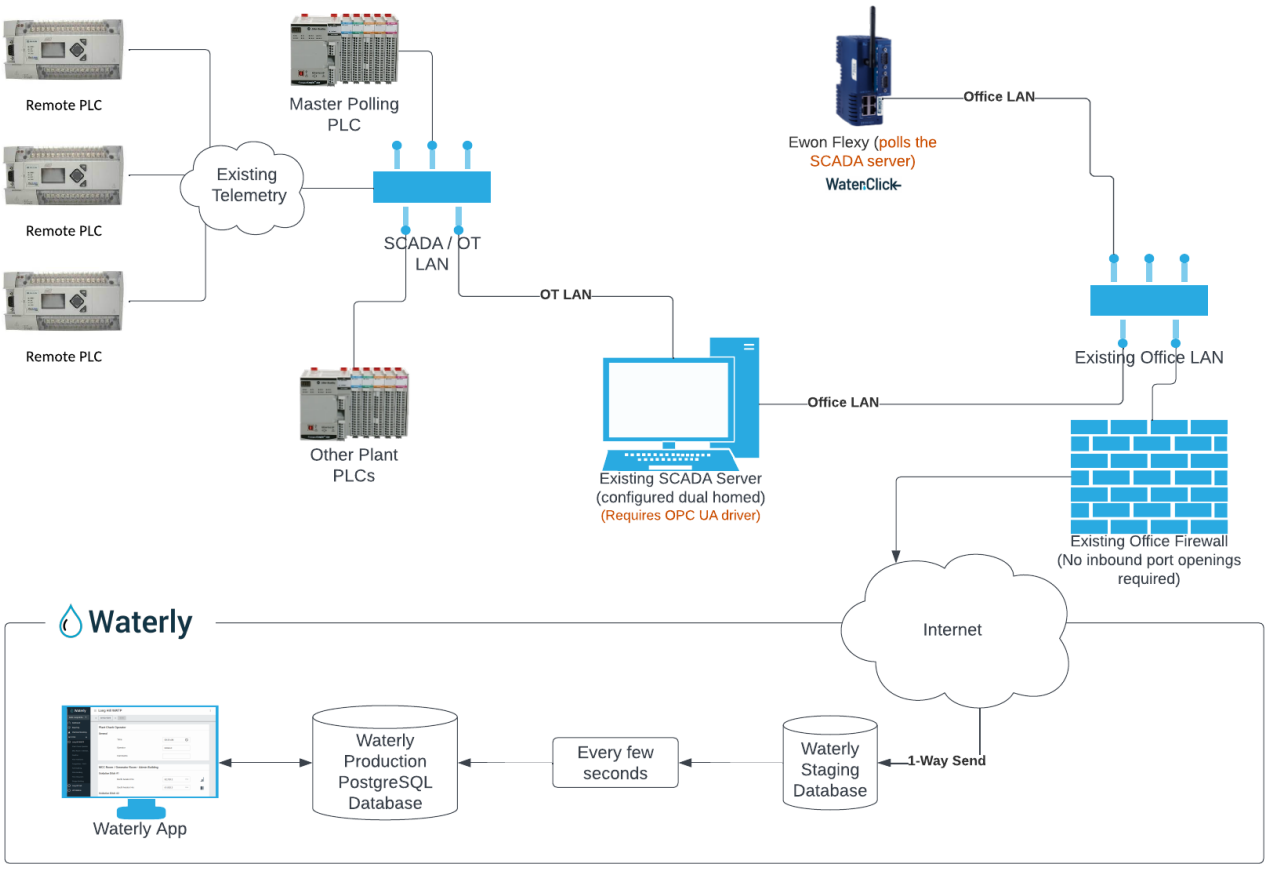
Waterly utilizes HMS Ewon's Flexy device for SCADA connectivity. There are three primary options for our customers use. OPTION 1 typically provides better redundancy (in that the SCADA server can be unavailable and you'll still have Waterly data flowing to the cloud), OPTION 2 can provide a more secure cybersecurity posture (in that the PLC does not "see" the Flexy remote data tool), and OPTION 3 pushes data directly to the cloud without touching any other IT infrastructure.

BOTH OPTIONS REQUIRE THAT

Option 2 requires that the SCADA server has The two options are shown visually below:

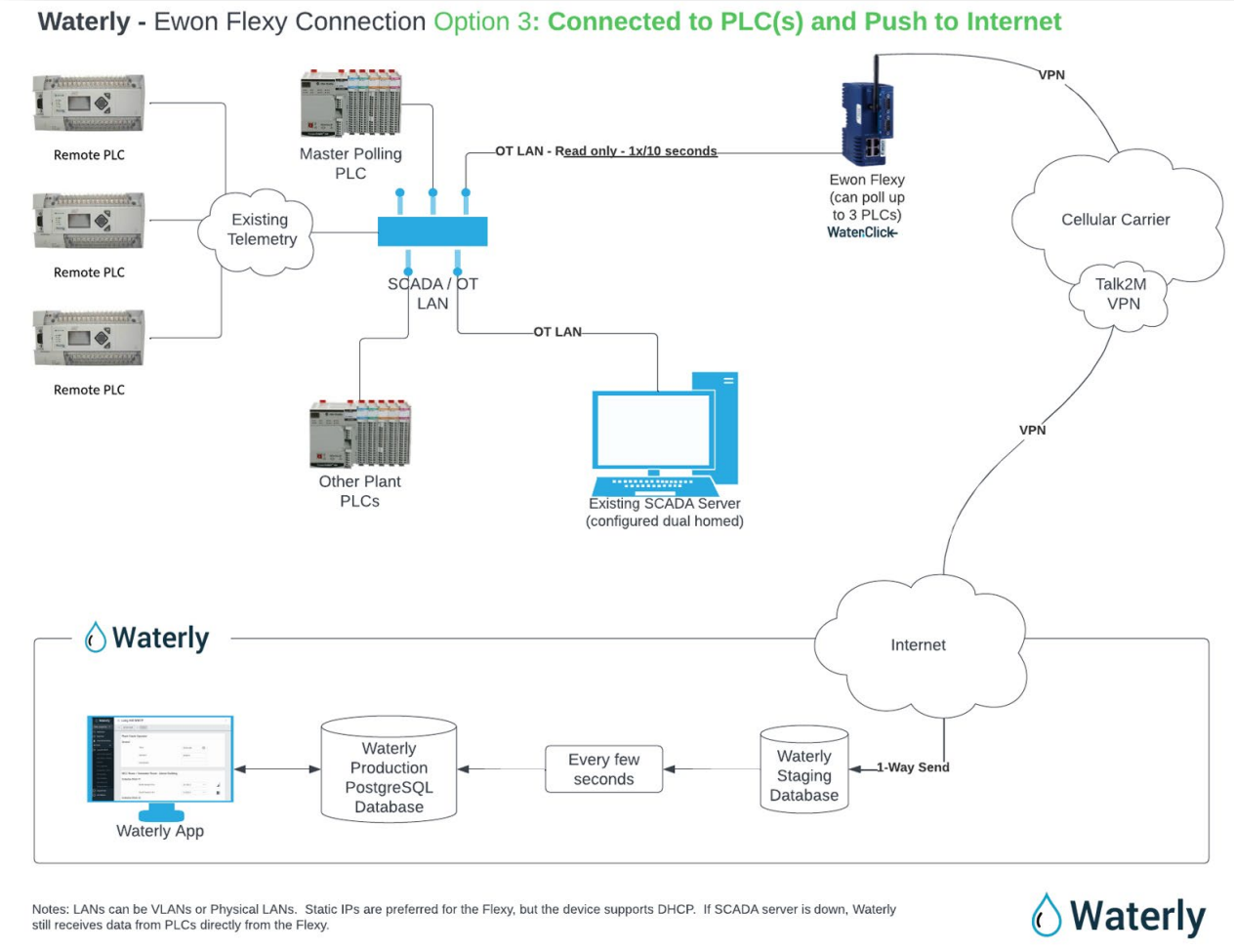


Waterly - Ewon Flexy Connection Option 2: **Single Interface - Connected to SCADA Server**



Notes: Flexy Polls the OPC UA Server (may require licensing for SCADA to support OPC UA). If SCADA server is down, no data can be transmitted to Waterly

Waterly



18. Are the URL's for the service well defined as to allow URL/Firewall access in restricted environments?

For Waterly's services:

app.waterlyapp.com (the Waterly app)
***.waterlysoftware.com**
***.waterly.com (our email)**
waterly.freshdesk.com (our Support Helpdesk)

For the Flexy services: If the customer firewall rules can be based on DNS names, our recommendation is to whitelist *.talk2m.com. If that is not possible, HMS Ewon publishes an IP page, that will need to be tracked when changes are made from time to time.

From that, we see the following list currently:

Hostname	IP	Ports
device.api.talk2m.com	92.52.111.213	TCP 443
device.vpn28.talk2m.com	169.60.86.33	TCP 443 UDP 1194
device.vpn32.talk2m.com	50.56.154.221	TCP 443 UDP 1194
device.vpn35.talk2m.com	18.229.200.159	TCP 443 UDP 1194
device.vpn37.talk2m.com	198.23.64.129	TCP 443 UDP 1194
device.vpn43.talk2m.com	184.173.179.89	TCP 443 UDP 1194
device.vpn50.talk2m.com	161.47.81.213	TCP 443 UDP 1194

19. Are Terms of Service or Service Level Agreement (SLA) details available addressing the following:

A. Affirmation of the ownership of the data, and our rights to the data

Customers own their own data and consequently, can use data as you please. You have access to download all of your data at any point without contacting us. We can, however, use your data for our own purposes, provided that we strip/remove/anonymize your data before doing so. We do not sell or give data marked as yours to anyone.

B. Infrastructure and security standards maintained by the service provider

Sorry, our T&Cs do not directly address this at this time.

C. Our ability to audit or review audits of the compliance to security standards

You are welcome to review any of our infrastructure setup/design at any point.

D. Enumerated rights and costs when discontinuing the service

Customers have full access to all of their data if there is a termination of service with us. We won't make you pay to get anything back and will only owe for the current period you are paying for.

WaterClick Partner - Ewon Flexy Specific Device questions

1. What is the specific model you provide?

We provide the Ewon Flexy 205 with the most current firmware at time of delivery.

2. **How are system updates applied?**

   They are patched prior to shipping with the most recent firmware. In-place updates are periodically done in the event of new firmware/software/updates.

3. **Since this is an IoT platform device, are there applications that run on the device that need to be maintained/updated?**

   There are not any other applications that run on the device that need to be maintained or updated.

4. **What is the expected supported life cycle of the device hardware and software?**

   5-10 years. We would ship a new device at no additional cost if there was a required hardware update.

5. **How does Waterly manage the device via the outbound only connections?**

   Device-initiated 100% encrypted/VPN connection.

6. **Is the network traffic well defined, as to be able to create precise firewall rules both out to the internet and internal to the protected SCADA environment.**

   Yes, very well defined. Our technical support can provide details before it is shipped if custom outbound firewall rules are requested. No inbound firewall rule is required, as there is no inbound traffic.

7. **Are there alternatives to giving the Flexy application direct access to the PLC? Internal data collector that replicates to an separate internal location the flexy can poll?**

   Yes. You could create a new DMZ for the Flexy off of a firewall and create a dedicated ACL for the Flexy and then another strict set of rules to allow it to route outbound only. Or you could create a separate server in a DMZ that ran an OPCUA driver like **KepWare OPC Suite**. That would be another small VM to run, but you could isolate the Flexy on the same LAN as the OPC Server, effectively creating a outbound/cloud facing data stream separate from SCADA. The OPC driver is about $1600 or so for a perpetual license or $600/yr, but now you have another Windows OS to patch and manage. At the extreme end of the spectrum, some of the largest utilities in the US use **unidirectional OT gateways**, but you would be looking in the $50k-150k range plus support. 😬 We are happy to discuss these options, if needed.