tether

Tether Technology -

The IOT Gateway for Cloud access of your on-premise devices

www.tetherit.io

info@tetherit.io

+44 (0)208 099 6260

Tether Technology Ltd,
199 Bishopsgate,
London, EC2M 3TY

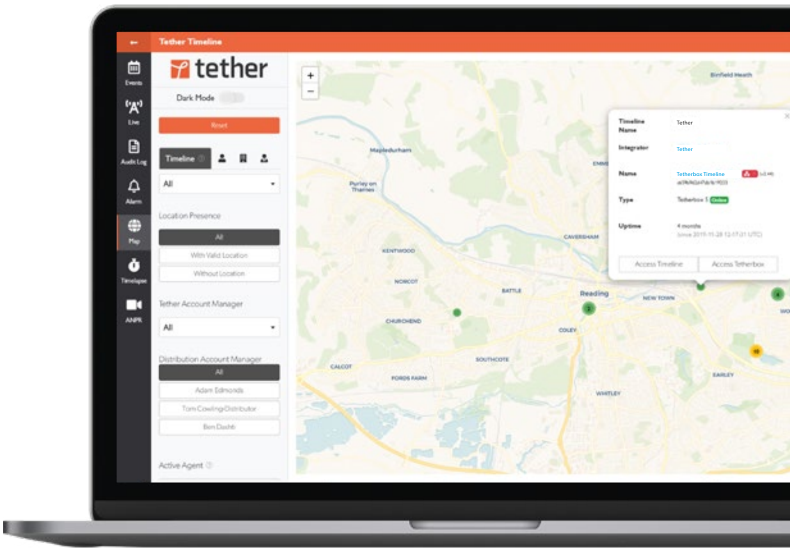
Solid Secure Straightforward

Executive Summary

Our world is changing more rapidly than we could ever have envisaged. Operating remotely is becoming the new normal and managing multiple properties ever more challenging. Equipment at these properties keeps them secure and operating but these devices are themselves vulnerable and need monitoring and updating.

It is very difficult to keep devices secure as it often involves driving to site, physically connecting to the network, performing firmware updates or configuring complex VLANs. Worse yet, the newly updated firmware can be out of date by the time the engineer leaves site.

In this document we outline how Tether is different, how we drastically reduce the need for on-site engineers, what measures we take to ring fence your devices and how we provide secure, remote access to them.



Timeline Name: Tether
Integrator: Tether
Name: Tetherbox Timeline
Type: Tetherbox 5 Online
Uptime: 4 months

Timeline: All
Location Presence: All
Tether Account Manager: All
Distribution Account Manager: All
Adam Edmonds
Tom Cowling-Distributor
Ben Dasht

About Tether Technology

Tether Technology is a Secure, true Plug and Play IOT Gateway that provides remote access, monitoring and support for any on-premise devices such as: CCTV, alarm, access control, solar / fuel cell health or information display devices. At Tether we think about your security beyond just creating a secure product.

We think about how the product will be used in practice and what other tools will facilitate a more secure deployment long term. As a result, the breadth of devices we connect expands constantly.

Suspicious Access Detection

Cloud Communication via Secure VPN

All changes are done Centrally

Geolocation, Device & ISP Detection

Secure Offline Access for Emergencies

Automatic Security Updates

Secure local streaming

Access via API & HTTPS

All Access is Audit Logged

Solid Secure Straightforward

tether

Benefits at a Glance

Tether Technology, was established in the UK in 2009. At Tether, we take your security very seriously. We designed the platform to operate in the most secure and demanding environments. We are deployed internationally across multiple sectors including: financial services, healthcare, education, retail, hospitality, housing associations and care homes.

	Traditional	**Tether Technology**
Health Monitoring	No way to tell if a device is operational	Health monitoring of all devices and notifications
Data Transmission	Insecure transmission or reliance on VLANs or custom VPNs	HTTPS/VPN is used for all data transmission
Firmware	Site visits & manual firmware updates	Over the air updates, with meaningful functional improvements
Data Storage	On site storage vulnerable to failure	Solid-State Edge and cloud storage
Network Setup	Requires opening port for inbound connections	Outbound connections only, usually no network changes needed
VPN	Requires expensive VPN or MPLS	VPN built into the product
Remote Access	Unsafe remote access	Two-factor authentication, full minute by minute audit log
Credential Management	Credentials are kept in printed documents / spreadsheets and shared insecurely	Every user has a single login to all sites they have permission to access
Remote Provisioning	No remote provisioning	Ability to securely tunnel to any device to remotely provision, with a full audit log
Configuration Management	Configuration is stored on the unit and lost if the unit is lost or stolen	Ability to migrate configuration between units or to push configuration to 100s or 1,000s of devices
Default Configuration	Un-secure by default	Secure by default and automatic setup that suits 99% of installations

Solid Secure Straightforward

How Tether Technology communicates

Our solution comprises a Simple to Install device on-premise - **The Tetherbox**, together with our platform - **The Tether Cloud**. All communication between your Tetherbox and the Tether Cloud is done via a VPN with SSLv3 certificates using 4096 byte sized keys, each connection is challenged to reauthorised once a week.

Each certificate can be revoked if we detect a Tetherbox is cloned or we detect any suspicious traffic. All communication is encoded into 'msg packs' using tokens and sent through a secure MQTT message broker. These safeguards protect against MITM (man in the middle) attacks, MAC spoofing and other types of attacks.

Data Flow

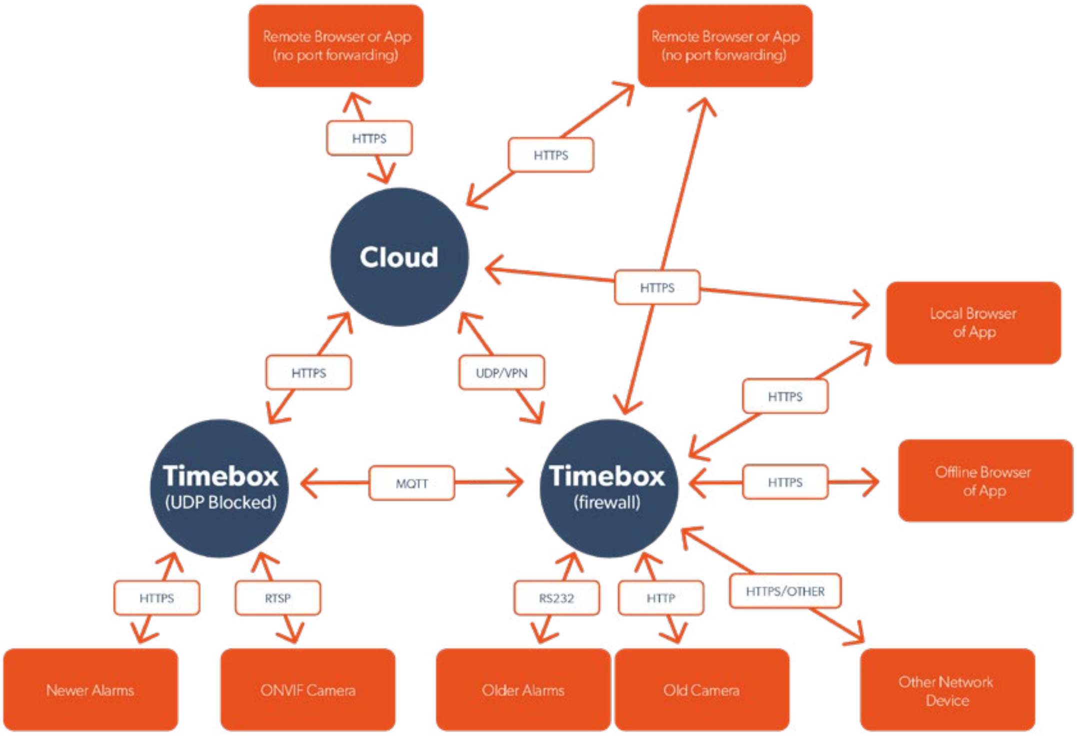
The information data flow can be complex, but is largely hidden from the end user. The Tether Cloud will generate HTTPS certificates for every lan IP, external IP, VPN IP of each Tetherbox, so that every device can communicate reliably and securely. By utilising a message queue for all communication, we ensure that no data is lost, even during prolonged periods of offline operation.

The diagram on below is an partial representation of data flow:

Tether Cloud

The Tether Cloud is designed to scale horizontally and every sub-system has redundancy built in including:

- Database servers
- Application servers
- Live playback servers
- Message handling servers
- Provisioning servers
- Load balancing servers
- Monitoring servers



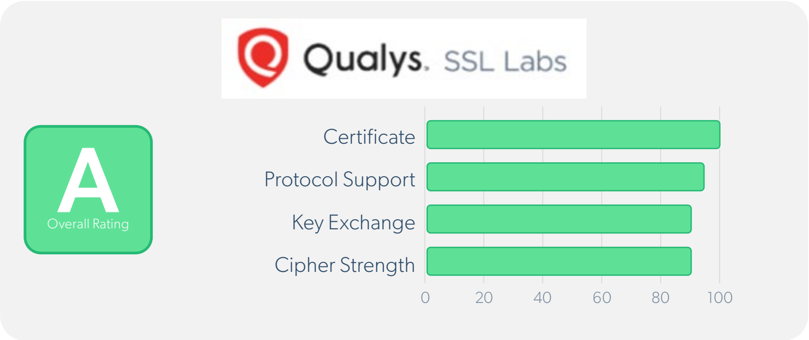
How you access

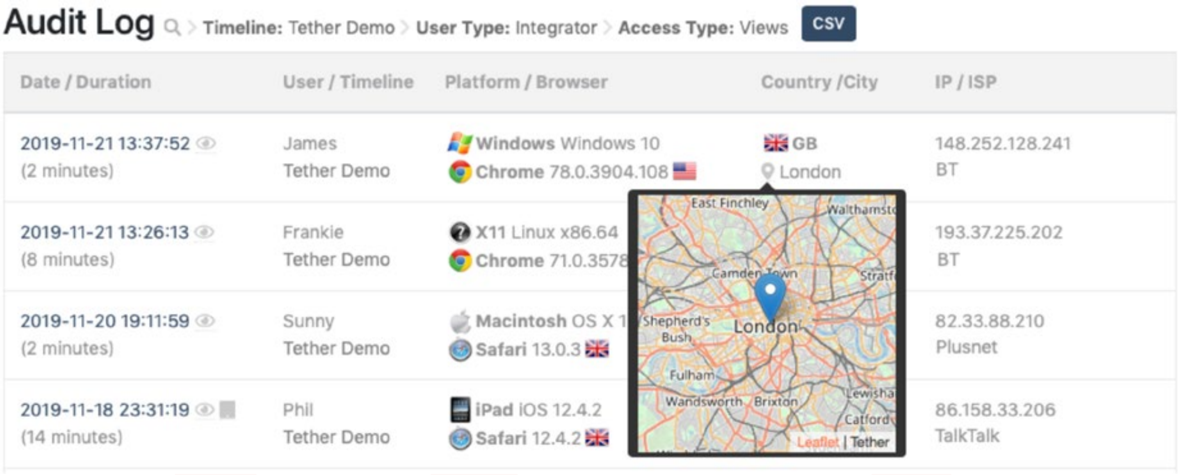
All access is done either via an API (e.g. control rooms or CMS applications) or using a web browser (HTTPS). The application has safeguards against many types of attacks, including Cross-Site Request Forgery (CSRFs), Self-contained XSS, Brute Force, Account Hi-Jacking and many other types of attacks.

Every single request goes through two layers of auth and auth (authentication and authorisation) which includes a full audit log of all access and changes. Even a single snapshot from a device is subject to this security. No access or changes are possible without going through these layers.

The audit log in the system also geolocates every request, discovers details such as the Internet Service Provider of the person accessing, what hardware they are using, what software they are using (for example, an iPhone 11 Pro using Safari from a BT connection in London, England). Using this information, the system can make intelligent decisions when any access is deemed "suspicious" e.g. access from a new city.

When using intelligent local streaming, temporary tokens are generated for each accessing user in order to pull live and recorded events directly from the Tetherbox.





Audit Log > **Timeline:** Tether Demo > **User Type:** Integrator > **Access Type:** Views CSV

Date / Duration	User / Timeline	Platform / Browser	Country /City	IP / ISP
2019-11-21 13:37:52 (2 minutes)	James Tether Demo	**Windows** Windows 10 **Chrome** 78.0.3904.108	GB London	148.252.128.241 BT
2019-11-21 13:26:13 (8 minutes)	Frankie Tether Demo	**X11** Linux x86.64 **Chrome** 71.0.3578		193.37.225.202 BT
2019-11-20 19:11:59 (2 minutes)	Sunny Tether Demo	**Macintosh** OS X 1 **Safari** 13.0.3		82.33.88.210 Plusnet
2019-11-18 23:31:19 (14 minutes)	Phil Tether Demo	**iPad** iOS 12.4.2 **Safari** 12.4.2		86.158.33.206 TalkTalk

Tetherbox Provisioning & Security

Each and every Tetherbox is provisioned and kept secure by Tether. There are no firmware updates to install. To increase the security of your Tetherbox, we recommend placing it out of sight and with no easy physical access to the unit.

The following ports are only used to make an **outgoing connection:**

Required:

- TCP port 443 (HTTPS)
- DNS (port 53)

Optional:

- UDP ports 1194, 1195, 1196 or 1197

The Tetherbox will make a connection to our cloud, hosted by 2 providers with the following IP ranges:

- Amazon: *https://bgp.he.net/AS8987#_prefixes*
- Linode: *https://bgp.he.net/AS63949#_prefixes*

On Premises Modes

Certain applications (such as some videos) are required to never leave the premises, we have various modes for this including:

- Limiting live view to only work on-premise, globally, or for specific users
- Limiting access to recorded video to on premise viewing or recording only

The advantage of these modes is you still get the management, audit log and health monitoring benefits of the cloud, without risk of actual images or video being accessible remotely.

Data Centre Security

All data-centres used by Tether are chosen carefully to meet all the following standards:

- **ISO 27001** - Provision of physical security, power, space and cooling (certificate available on request)
- **ISO 9001** - Design, construction, operations and infrastructure management of neural data centres, co-location services and other associated services (certificate available on request)
- Located in the UK
- Optional Cloud Storage in EU

Firewalls and Anti-Malware Recommendations

We do not make any specific recommendations for what Anti-Malware Software and Firewalls you should use on the device you use to access the Tether platform. As long as you have a modern web browser or a modern mobile device or tablet, the system will operate correctly and securely.

If you suspect that unauthorised third parties may have access to your laptop or any other device, please seek independent advice as this falls outside of the scope of this document.