tether

How Tether safeguards your physical security devices

Security Whitepaper (Q4 2021)

Tether Technology Ltd
info@tetherit.io
+44 (0)208 099 6260

Tether Technology Ltd
EPIC, White Rock Business Park,
Waddeton Close, Paignton,
Devon, TQ4 7RZ

Solid Secure Straightforward

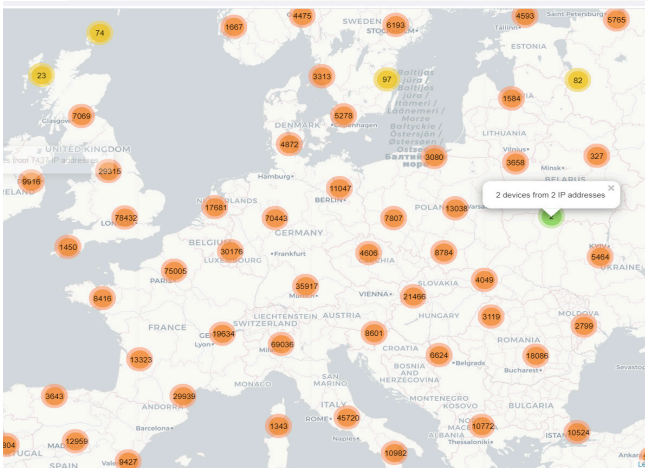
Executive Summary

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.

Every month, there is a new exploit, new discovered bug, or some vulnerability that leaves your on-premise devices open to unauthorised access. As an illustration, the map on the right comissioned by WHICH in Aug 2020 shows 3.7m hacked or vulnerable security devices across Europe.

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 Worse yet, the newly updated firmware can be out of date by the time the engineer leaves site.

Aug 2020 Map Showing 3.7m Vulnerable Security Devices



Source: https://hacked.camera/map

This document outlines 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.

About Tether

Tether Technology was founded in 2009 with the mission to **monitor**, **manage** and **maintain** physical security device with a **solid**, **secure** and **straightforward** platform and app. Tether unifies CCTV, alarm, access control as well as other relevant devices including routers, relays, solar devices and more.

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.

Highlights include:

- Suspicious Access Detection
- Cloud Communication via Secure VPN
- All devices are provisioned 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

tetherit.io
sales@tetherit.io
+44 (0)208 099 6260

Benefits at a Glance

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, banking, healthcare, education, retail, hospitality, housing associations and care homes.

	Traditional	Tether
Health Monitoring	No way to tell if a camera is operational	Health monitoring of all devices and notifications
Data Transmission	Insecure video 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, updates frequently bring meaningful functional improvements
Video Storage	On site storage vulnerable to failure	Solid-State storage as well as 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

tetherit.io
sales@tetherit.io
+44 (0)208 099 6260

How your Tetherbox Communicates

Our solution comprises an on-prem device called **Tetherbox**, which connects to the **Tether Cloud** platform.
All communication between your Tetherbox and the Tether Cloud is encrypted through a VPN with SSLv3 certificates using 4,096 byte sized keys. Each connection is challenged to be 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

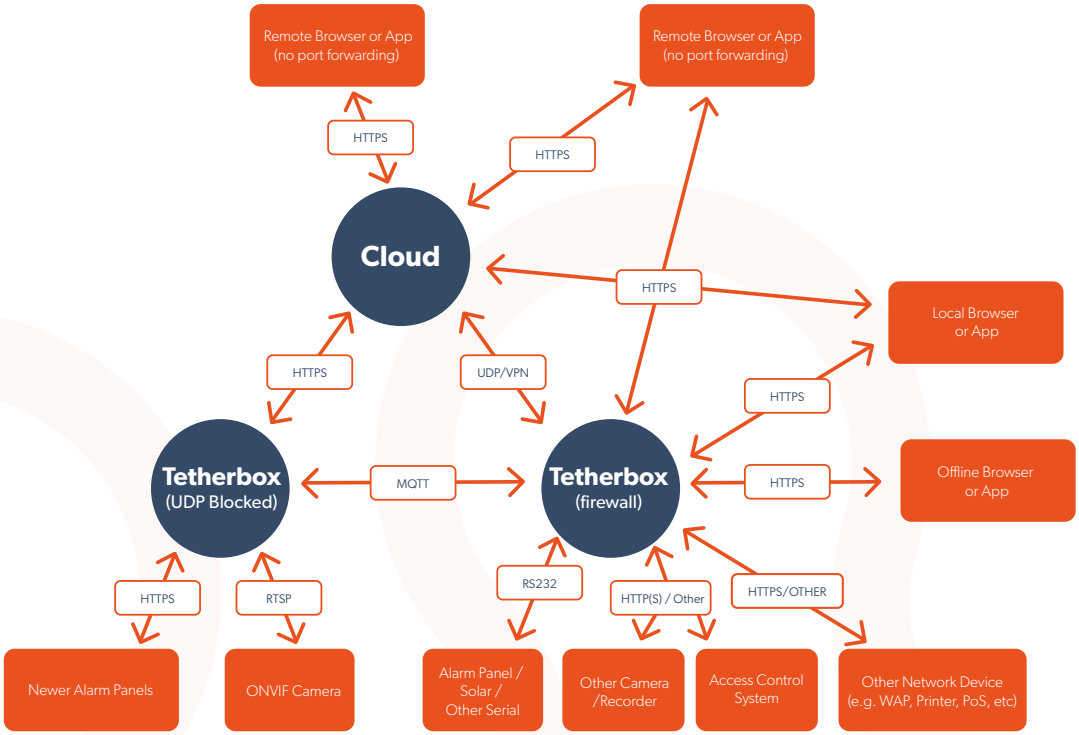
The information data flow can be complex, but is largely hidden from the end user. The Tether Cloud will generate HTTPS certificates for every LAN IP, external IP and VPN IP of each Tetherbox, so that every device can communicate reliably and securely. By utilising a message queue for all communication,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

The diagram below is a partial representation of the data flow:

Tether Cloud

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
- Other miscellaneous



How You Access

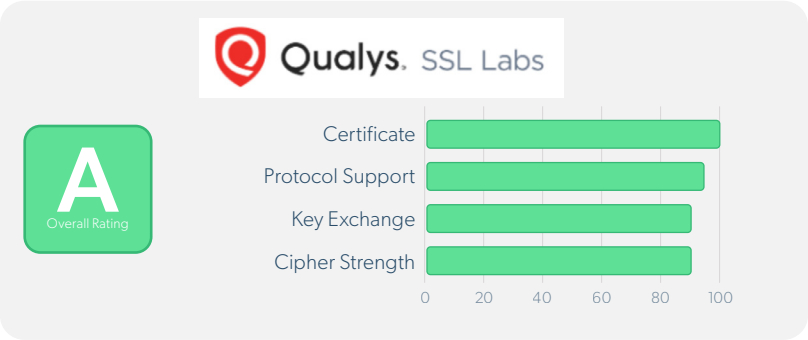
All access is done either through a website, through our native iOS or Android apps, or through an API (e.g. alarm receiving centres or custom applications). **You do not need to install any applications or plugins to use the Tether platform.** Two-factor authetication is also supported.

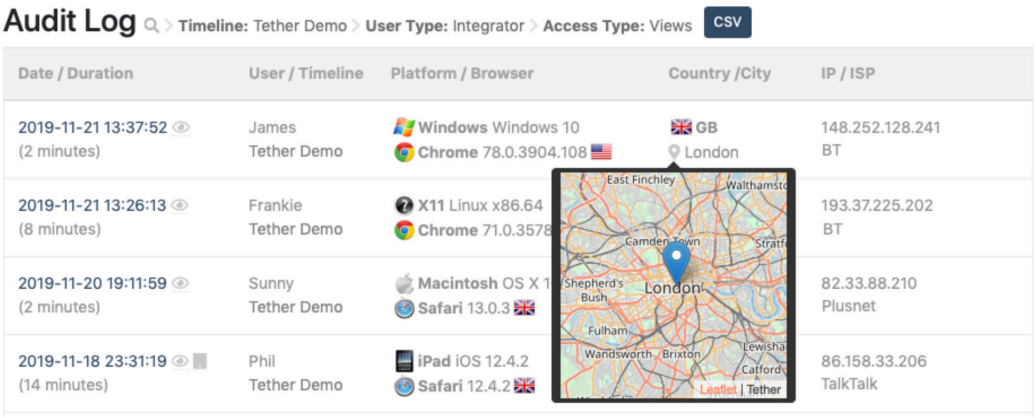
The web and native applications have safeguards against many types of attacks, including Cross-Site Request Forgery (CSRFs), Self-contained XSS, Brute Force, Account Hi-Jacking and many other types of attacks.

Every single request goes through two layers of 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 12 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.





tetherit.io
sales@tetherit.io
+44 (0)208 099 6260

How Tetherbox Connects and is Kept Secure

The Tetherbox makes an outbound connection to the Tether Cloud. We prefer to use UDP for performance, but if this is not available, port 443 is used to emulate HTTPS traffic. As long as a person on site can access google.com, Tetherbox should also be able to connect without port forwarding or any other changes to the network.

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

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-Premise Modes

Certain environments require that video never leaves the premises, so we have various mode to accomplish this:

- Limiting Live View to only work on-premise, globally, or for specific users.
- Limiting access to recorded video to on-premise viewing only.

The advantage of these modes are that 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 the UK or the 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.

tetherit.io
sales@tetherit.io
+44 (0)208 099 6260

Frequently Asked Questions

- **Is Tether a multi-tenant cloud?**

Yes. The original Tether design had a separate instance per customer and many products on the market still follow this traditional approach.

Separate instances meant higher downtimes (compared to a load balanced high availability infrastructure of a true multi-tenant cloud), slower security update rollouts (compared to an always up to date cloud service), audit and health reports were separatate per site (instead of a single global report), users had to be added multiple times to different instances (instead of a single central permission system), each site had to be added separately on every user device (instead of logging in and seeing all allowed sites/devices), every site had to be set up individually in a control rooms (instead of adding all sites with a single API request) and more.

In 2014, Tether have made the decision to design a secure and scalable multi-tenant cloud, which has taken 4 years to bring to market. It is the modern approach taken by modern web platforms and brings significant advantages to the traditional single-tenant deployments.

- **Can data be exported?**

Yes. There are several ways to export data from the platform, either by generating a link to a specific event(s), exporting configuration and other metadata in CSV or Excel formats, downloading video surveillance in MP4 format and more.

- **Do I need to install any software?**

No. While we do offer native applications for iOS and Android, they are optional and the platform is fully usable through the web application.

You can login at https://tetherit.io

- **Who has access to the platform?**

Every user is added by a designated admin and managed centrally. The admin can give user permission to access specific sites or devices (e.g. cameras). A central read-only audit log is kept which can be viewed online or exported in Excel format.

The platform also has "support access" if required. Once support access permission is enabled by you, your integrator, as well as Tether Technical Support if required, can access and assist with any issues. You will be prompted to disable support access in normal use.

- **Has Tetherbox and Tether Cloud been audited?**

Tether have a professional penetration tester on staff who audits all code as well as runs both automated and manual penetration testing monthly. This includes using tools like Nessus and SSL Labs (reports available on request).

We welcome any and all security audits.

- **Where and how is video data stored?**

Video data is either stored locally on your Tetherbox, or optionally it can be backed up to the Tether Cloud. Tetherbox stores the raw video data without any modifications to ensure the evidence is legally admissable. Tether can and does transcode video for lower latency / quicker previewing over the Internet without modifying the original recorded footage.

Tether also sends SHA1 checksums of every 1 minute of footage, which can be used to prove in court that evidence was not tampered with.

tetherit.io
sales@tetherit.io
+44 (0)208 099 6260