BUFFALO™

Secure sensitive information and better protect your business

Network Attached Storage Solutions from Buffalo Americas Adds an Extra Layer of Defense

Security is top of mind these days—and for good reason. Losing sensitive data due to theft or damage to a physical device can crush an organization. At the same time, cyberattacks have become more frequent and sophisticated, forcing organizations to proactively protect hardware and information assets. And, if you're in certain industries, like healthcare or financial services, you're also under pressure to secure information to better meet compliance mandates like HIPAA compliancy and avoid hefty fines.

Creating a data replication and backup strategy is a critical first step, which is why many businesses employ NAS solutions. But there's more that you can, and should, be doing—and Buffalo Americas can help. We build multiple layers of physical and digital security into our solutions that help you better protect your hardware assets and the valuable information stored on NAS devices. Here are some of Buffalo's security solutions that will help strengthen your security posture:

LOCK DOWN HARDWARE ASSETS WITH PHYSICAL SECURITY MEASURES ON BUFFALO DEVICES

- **Kensington Lock**

Many of Buffalo Americas NAS devices include a Kensington slot that lets you cable your NAS device to a particular location, preventing removal.

- **Front Panel Lock**

The front panel lock included on our TeraStation desktop products helps prevent users from removing or stealing the hard drives housed inside.

- **Boot Authentication**

This security measure requires users to authenticate—via password or authentication server before the system boots up and information on the hard disks can be read. This helps prevent information from becoming compromised. Boot authentication is currently available on TeraStation™ 3010 and 5010 series NAS devices only.

SAFEGUARD INFORMATION STORED DIGITALLY

- **AES 256-bit encryption (Advance Encryption Standard)**

Information stored on hard drives is encrypted until proper authorization is received. An additional deterrent when encryption is enabled prevents one NAS device being used in another if removed or stolen.

- **Ransomware solutions**

Prevent hackers from holding your information hostage. Buffalo TeraStations enable you to disable sharing and establish read-only permissions as part of your back-up solution. This way you can still access backed-up information in case of a ransomware attack.

- **Optional: Trend Micro Antivirus**

The NAS Security anti-virus service can scan files on a scheduled basis and can even scan files in real-time, protecting the data on the TeraStation from the threat of virus.

Don't risk having sensitive information stolen or destroyed. Fortify your security strategy with an additional level of protection you can only get with Buffalo NAS devices