RIMAGE®

Avoiding Malicious USB-Sticks with RIMAGE® RX400 MedX

USB-Sticks are a widely used medium by many people and employees in companies. Due to the small form factor, and the enormous storage capacities, they allow easy and convenient exchange and transport of data. For this reason, USB-Sticks have become an indispensable part of today's life.

Of course, this carries the risk that unknown elements can be infiltrated into a company network via the USB-Stick. Since the USB-Stick is used within the network, by plugging it directly into the workstation, it bypasses the company's virtual perimeter defense. All these factors make it a very convenient attack tool for cybercriminals. They use „malicious" USB-Sticks that contaminate and infiltrate networks

With the Rimage RX400 MedX System and our dedicated USB-Sticks, we provide a simple and effective method to minimize the threats of „malicious" USB Sticks.

The RX400 approach

One of the most important things to avoid "malicious" USB-Sticks in your company is to provide training to your employees and create awareness of the possible risks of insecure USB-Sticks.

The Rimage USB-Sticks for the RX400 MedX have a special security feature called WORM (Write Once, Read Many) and are the only USB-Sticks you can use in the RX400 MedX system. Each stick will be already WORM protected when delivered to the customer, disabling the possibility of adding data by a none-authorized system or individual. This prevents the possibility of easily adding any files that may contain malware, viruses, or any other threats.

Recording Data: only in RX400 MedX
Reading Data: everywhere

Only with the RX400 MedX system you are able to unlock the WORM USB-Stick, add new data, and re-enable the WORM protection afterwards. This limits the risks of malicious USB-Sticks and provides an additional IT Environment protection.

OVERVIEW RIMAGE USB-STICKS

To provide you the best USB stick in value for money, we created two Patient USB sticks - one for a single time use and one for multi use. In order to ensure a closed and secure enviroment, we are limiting the USB sticks that can be used with the RX400 MedX to limit and avoid any threats (virus, malware, ...) from unknown media.

TopLine Patient USB-Stick (64GB)
BaseLIne Pro Patient USB-Stick (16GB)
USB Version: 3.1
MultiWORM Feature
Connector: USB A
Max Read/Write Speed: 400/200 MB/s
Sequential read/write: 40/30 MB/s
Data Retention Time: up to 10 years

BaseLine Patient USB-Stick (16GB)
USB Version: 2.0
SingleWORM Feature
Connector: USB A
Max Read/Write Speed: 200/100 MB/s
Sequential read/write: 25/8 MB/s
Data Retention Time: up to 3 years

RIMAGE® RX400 MedX

Do you know WORM?

While the ability to rewrite is often considered a primary feature of a USB-Stick, there are many cases where it is undesirable, and may even make USB-Sticks inappropriate for a specific task. With the Rimage RX400 MedX WORM feature, this is no longer a concern. Protect a stick from malware, ensure the longevity of the data or use it for legal or compliance reasons with certainty that the data is safe from unauthorized alteration.

Write Once, Read Many

Write once, ready many is often shortened to the acronym WORM and is typically associated with optical devices like CD or DVD. This refers to the ability to protect a device to prevent it from being written to more than one time, while allowing it to be read many times.

While USB-Sticks are normally thought of as being completely re-writable, with the WORM feature, RX400 MedX USB-Sticks are automatically locked after writing to prevent any further writing from uncontrolled sources.

Why WORM?

The primary advantage of using WORM on a USB-Stick is to prevent unintended modification (either accidentally or maliciously modified) of the data written to the device. This protects the data originally recorded to the device from being infected by malware, accidentally deleted during use or corrupted by unexpected power loss to the device.

Many security policies restrict the use of USB-Sticks on computers due to the risk of them spreading malware, but a device recorded with the WORM feature can be used without the normal risks if the recorded data has been provided by a secure and trusted source.

In addition to protection from malware, WORM can offer protection for files for compliance and legal standards. For legal documents, law enforcement evidence or other critical information, WORM ensures that the data will not change after recording. This is crucial for chain of evidence and other compliance guarantees.

Protection of the data includes ensuring the highest longevity of the data on a device. NAND flash memory, which most USB storage devices are based on, has a limit on the number of times each memory cell can be written to. As these cells get re-written, the cell becomes less able to store the data reliably.

By only writing to the drive once, and preventing further writing, WORM ensures that the data will be readable on the device for the maximum amount of time.

How does it work?

The WORM feature is already activated on the Rimage USB-Sticks but if needed it is re-activated in the Rimage RX400 MedX system and will be added to a device that is produced on the system.

The RX400 MedX system sends a command to the USB controller of the device, locking it on a hardware level. This will prevent all further attempts to write, modify or erase data on the device. Being locked at the hardware controller level means, that typical bypasses such as formatting the device, are not possible. Using alternate operating systems to access the device will not bypass the WORM protection.

CONTACT INFORMATION

Rimage Europe GmbH
Wernher-von-Braun Str. 9
63303 Dreieich-Offenthal
Germany

+49 (0)6074 8521 0

Sales@rimage.de

RIMAGE® RX400 MedX