Trivalent Provides Next Generation Data Protection on Rugged Devices

Case Scenario: Military

Challenge

Military branches rely on ruggedized devices for mission critical and covert communications in high-risk or hostile military operating environments. Although field operators may have limited or no network connectivity, they must still be able to securely store and access sensitive data, in runtime, on the device.

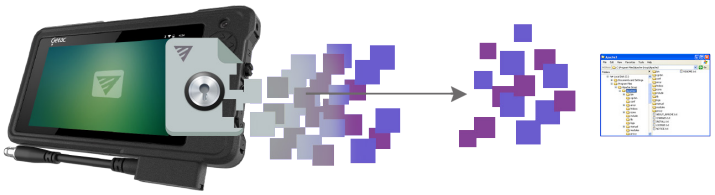
Commercially available and traditional endpoint security is not sufficient. The data protection solution must meet rigorous NSA security requirements to minimize exposure of classified or sensitive data.

Solution: Trivalent Protect

Trivalent Protect is the only NSA Commercial Solutions for Classified (CSfC) certified data-at-rest (DaR) solution. It is developed exclusively with the warfighter in mind to securely handle Top Secret and below data.

The Trivalent Data Protection Process

Trivalent's unique process of encryption, data shredding, secure storage, and authorized file reconstitution ensures that only authorized users can access the secured data.



Devices accessing critical data

Store Secure Shreds

1 **Encrypts** files as they are saved to disc

2 **Shreds** the encrypted files for storage

3 **Stores** the shreds across the device file directory

4 **Recombine** the shreds and decrypt for authorized user

Trivalent Protect

- **Security always stays with the data**. Both at rest and runtime.
- **Authorized data usage.** Only authorized users can access their secured data whenever needed.
- **Data Shredding.** Data is transformed and rendered useless to unauthorized users.
- **Easy to deploy and seamless.** Integrates seamlessly with other mission essential applications and with existing end-user workflows.
- **Supports Windows and Android**

www.trivalent.co 443-472-6712 sales@trivalent.us.com

Trivalent Data Protection Benefits (con't)

- **Does not require network connectivity.** Developed to provide data security and policy enforcement for the warfighter across multiple operational boundaries, in both dismounted and disconnected operations.
- **Groundbreaking and operator-friendly.** Patent-pending solution incorporates tactical operator feedback from live implementations to meet warfighter requirements.
- **Centrally Administered for service efficiencies.**

Case Scenario

Data Compromise during Operation Red Wings

In the Kunar Province of Afghanistan, Coalition Forces launched Operation Red Wings [1]. Part of the mission of this highly sensitive operation was to disrupt hostile local anti-coalition activity.

A four-man Navy SEAL reconnaissance and surveillance team was dispatched to gain intelligence on key personnel to assist with upcoming operations. The team relied on a mobile ruggedized device to collect and store critical data and to communicate back to their command.

Shortly after insertion, the team engaged in a ferocious firefight, which ultimately took the lives of three brave SEALs. Unfortunately, the insurgents were able to capture the SEALs' weapons and equipment. Their seized equipment included operational items such as weapons, night vision goggles and their ruggedized laptop. The laptop contained classified and sensitive information that the enemy could now leverage for hostile actions.

The insurgents proceeded to remove the hard drive. **Next they were able to successfully access the data from critical files that were on the laptop which contained the data**. Without authorized access, they could then easily view, use and distribute the classified and sensitive government data that was on the seized laptop.

Result: Next Generation Data Protection Must Always Stay with the Data

Military data requires security that stays with data at all times and can only be accessed by authorized users.

The added instrumentation of data security on the device makes a lost or stolen device worthless to the enemy.

[1] Operation Red Wings became the basis of the *New York Times* best selling novel and full-motion picture hit: "*Lone Survivor*"