Trivalent Provides Next Generation Data Protection on Rugged Devices

Case Scenario: Field Operations

Challenge

Remote or harsh environmental conditions require the use of ruggedized devices for Field Operations by many industries such as First Responders, Oil and Gas, Engineering, Law Enforcement, Border Patrol, Healthcare, Research and more. Mobile devices used in the field process sensitive, proprietary and critical information such as personal identifiable information (PII), schematics, trade secrets and more.

As new data exploits are released daily on mobile endpoints, traditional endpoint security is no longer sufficient. This is especially relevant in the field where devices are easily lost or stolen, network connectivity may be low and the need to store valuable data on the device is critical.

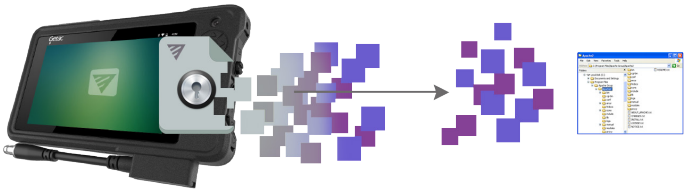
Organizations must consider a comprehensive data protection strategy for their ruggedized devices to mitigate financial loss and brand damage from the eventuality of a data breach or unauthorized access.

Solution: Trivalent Protect

Trivalent Protect enables security leaders to leverage military-grade security to protect their data on mobile endpoints.

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 Benefits

- **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.
- **Supports Windows and Android**

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

Trivalent Data Protection Benefits (con't)

- **Easy to deploy and seamless.** Integrates seamlessly with other mission essential applications and with existing end-user workflows.
- **Does not require network connectivity.** Developed to provide data security and policy enforcement 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 requirements.
- **Centrally Administered for service efficiencies.**

Case Scenario

First Responders

First responders routinely use ruggedized computing devices in the field. They are required to access, use and update critical or sensitive information, such as personal identifiable information (PII) or legal evidence, on these devices. Given the criticality of the data that resides on these devices, it is crucial that security remains with the data while it is at rest on the device and often in unconnected environments. Otherwise, protection hackers and unauthorized users gain access and use of the data for nefarious purposes.

The data security requirement on ruggedized computing endpoints is also underlined by strict organizational and industry compliance mandates, such as HIPAA.

Critical Infrastructure Field Operations (Energy, Utility, Transportation, Telecommunications)

Field engineers and operations personnel are required to access, manage and input new information in rugged conditions. For example, field personnel maybe required to review complex schematics on oil rigs or enter diagnostic data at remote stations. Network connectivity is not guaranteed and therefore the need for data to be securely stored locally is essential.

Security policies that support critical infrastructure requirements, such as SCADA, also require data protections that will thwart hackers and unauthorized users from accessing and using regulated and sensitive information.

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

Mobile devices used in the field require 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.