Trivalent Provides Next Generation Data Protection on Mobile Computing Devices

Case Scenario: Healthcare

Challenge

As the healthcare industry rapidly digitizes to provide increased access, better care, and more cost-efficient models, it has become a data rich and innovative industry. It is now characterized by new telehealth and outpatient care models, data-driven clinician and analytics software solutions and mobile computing devices.

New data exploits are released daily on mobile endpoints and commercially available, traditional endpoint security are no longer sufficient. This is especially relevant in telehealth, hospital, outpatient, and health insurance environments where devices are easily lost or stolen, network connectivity may be low, and the need to store valuable data on the device is **critical to patient safety and HIPAA compliance requirements**.

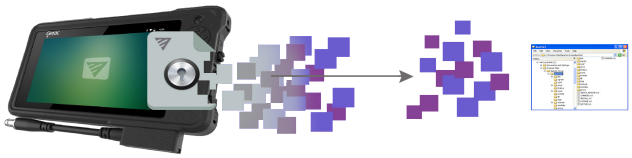
Information and security leaders must consider a comprehensive data protection solution for their mobile computing devices. This will help to minimize their risk profile, non-compliance penalties, mitigate financial loss and brand damage from the eventuality of a data breach or unauthorized access.

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 for 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

Telehealth and Health Insurance (Home Care, Outpatient, Eligibility)

Mobile computing devices are integral to the workflow of home care, remote outpatient clinicians and health insurance providers.

They all rely on mobile computing devices to access private and sensitive data, such as PHI, PII. They must also securely record and store new private information on their mobile computing devices while in the field; sometimes with no connectivity options.

Additionally, solutions are needed that protect field and confidential information if the device is lost, stolen or there is a data breach.

The need for data security that stays with the data is further underlined by strict data security and compliance mandates, such as HIPAA, that require critical and sensitive information is kept secure from unauthorized access and data usage.

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

Trivalent's next generation data protection technology uses a proprietary approach to provide unprecedented security that stays with the data regardless of network connectivity.

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

The Result: Your critical and sensitive data is **secure at rest** on mobile computing devices.

- This solution further enables the security team to reliably and quickly recover its data, even in the event of a breach or whenever needed (i.e., business continuity).
- End-users simply continue using their ruggedized devices without any changes.
- Trivalent's solution enables security teams to strengthen their Incident Response Plans with this new layer of data resilience. In turn, the risk of data loss that could yield financial and brand damage is minimized.