Trellix

DATA SHEET

Trellix® Drive Encryption

Highlights

- **Stop Unauthorized Access**
  Protect computers and laptops from data breaches.
- **Demonstrate Compliance**
  Report on encryption status of devices inside and outside the network.
- **Enable User Self-Service Recovery**
  Allow users to recover credentials without involving the help desk.
- **Centralize Management**
  Deploy protection, administer policies, and produce reports in a single console available on-premises or via SaaS.

Protect Devices from Data Breaches

The number of confirmed data breaches due to lost or stolen assets is rising— even on-site corporate devices are vulnerable to threats from malicious insiders. These breaches can expose personal, business, and financial information, resulting in penalties and financial losses for the organization. Implementing full disk encryption is one of the most effective ways to defend against these threats, ensuring sensitive data on devices remains protected.

Deployed from a centralized console available on-premises or SaaS, Trellix Drive Encryption offers proprietary, full-disk encryption protection for Windows workstations and laptops against brute-force attacks. With cryptography that meets FIPS 140-2 standards, Drive Encryption will protect the operating system and asset data from unauthorized access.

User Authentication

Manage user access controls from a central console. Grant or revoke access for specific users, and require authentication before the computer boot cycle. Integrated with Active Directory, Drive Encryption allows a single or multiple users to authenticate on a device.

Seamless Log-in Experience

Make it effortless for users to authenticate their access with a seamless log-in experience and single sign-on for Windows OS.

User Self-service Recovery

Reduce the amount of help desk support needed by empowering users to recover their credentials using a variety of methods, including challenge questions, a smartphone application, and a recovery portal.

Lost & Stolen Assets | Know the Numbers

- 91% of lost and stolen assets resulted in a data disclosure[1]
- 92% of threat actors involved in data disclosures were financially motivated[1]
- 200+ days on average to detect and contain a data breach[2]
- $1M in penalties paid by a healthcare provider for a single stolen unencrypted laptop[3]
- Personal information was the top category of information compromised when an asset was stolen[1]

Enhanced Security with MFA

Create passwordless login using a smartcard to enhance security and comply with NIST SP 800-111 recommendations for phishing-resistant authentication.

Compliance Reporting

Make your next audit painless by reporting on the latest state of encryption protection for devices and with an audit log that shows the last known access control activity for a lost/stolen device.

Trellix Native Drive Encryption

Do you have a mixed OS/device environment with macOS, bring-your-own-device, or devices that don't require user-based access controls? Trellix Native Drive Encryption comes with a purchase of the full Drive Encryption product, offering management for Bitlocker and FileVault protection in a single console available on-premises or via SaaS. Native Drive Encryption can help monitor for gaps in device encryption, rotate recovery keys, and automatically provision new systems. Choose the right level of encryption protection for your enterprise devices with the combined power of both Trellix Drive Encryption products.

Trellix Drive Encryption is available individually or as part of our Trellix Data Security Suites.

To learn more about Trellix Data Security Suites, please visit www.trellix.com/products/data-security-suites/.

To learn more about Trellix Drive Encryption solutions, please visit www.trellix.com/products/data-encryption/.

Sources

1. Verizon 2024 DBIR
2. 2023 Cost of a Data Breach Report (IBM)
3. Unencrypted stolen laptop costs Lifespan more than $1M - healthcareitnews.com