Trusted Cyber Technologies

THALES
Building a future we can all trust

CipherTrust Transparent Encryption Ransomware Protection

Challenge: Ransomware Blocks Access to Mission Critical Data

Ransomware has been on the rise since 2020. It accounts for 25% of all data breaches[1]. Ransomware attacks can bring business operations to a grinding halt by blocking access to critical data until a ransom is paid. A ransomware is expected to strike businesses and individuals every 2 seconds by 2031[2].

Baseline security practices using perimeter controls such as next generation firewalls, secure email/web gateways and focusing on closing vulnerability gaps alone have not been sufficient to prevent ransomware attacks. One of the main challenges for organizations today is to safe guard critical data from being encrypted by unauthorized processes and users on endpoints and servers.

Solution: CipherTrust Transparent Encryption Ransomware Protection

CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) provides a non-intrusive way of protecting files/folders from ransomware attacks. CTE-RWP watches for abnormal I/O activity on files hosting business critical data on a per process basis. It allows administrators to alert/block suspicious activity before ransomware can take hold of your endpoints/servers.

Key Advantages

- **Transparent Data Protection.** CTE-RWP continuously enforces ransomware protection per volume with minimal configuration and no modification to any applications on the endpoint/server. It continuously monitors abnormal file activity caused by ransomware infected processes, and alerts/blocks when such an activity is detected.

- **Easy to Deploy.** CTE-RWP enables administrators to start with ransomware protection alone, without setting up restrictive access control and encryption policies on a per file/folder basis, which is available in a CTE license.

- **Robust Ransomware Detection.** CTE-RWP uses process-based machine learning models to dynamically detect suspicious file I/O activity. It identifies and alerts or blocks ransomware on endpoints/servers. Approved processes can be added to a trusted list to bypass monitoring.

1 https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
2 https://cybersecurityventures.com/ransomware-will-strike-every-2-seconds-by-2031/#:~:text=Cybersecurity%20Ventures%20predicts%20that%20by,than%20ever%20protecting%20against%20ransomware

Licensing

CTE-RWP is licensed separately. It provides an adequate level of ransomware detection, without configuring detailed acess control policies at a file/folder level on each endpoint/server. Combined with a CTE license, administrators can additionally apply finer-grained access control and encryption. CTE-RWP can be licensed separately or in conjunction with CTE.

Additional Data Protection Against Ransomware With CipherTrust Transparent Encryption

Customers can maximize ransomware protection on their endpoints/servers, by adding a license for CipherTrust Transparent Encryption (CTE), to gain the following additional benefits not provided by CTE-RWP.

Fine-grained Access Control

- Defines who (user/group) has rights to encrypt/decrypt/read/write or list-directory where critical data resides
- Place strict access control policies around backup processes, including encrypting backups to prevent data exfilteration
- Guard point level trusted list of files (binaries) that are approved to access and encrypt/decrypt protected folders including signature checks on trusted applications to ensure their integrity.

Data at Rest Encryption

- Encrypt critical data, wherever it resides on-premises or in the cloud
- Make critical data worthless to intruders, since they cannot monetize encrypted data by threatening to publish
- Guard point level trusted list of files (binaries) that are approved to access and encrypt/decrypt protected folders including signature checks on trusted applications to ensure their integrity.

With MFA for CipherTrust Encryption

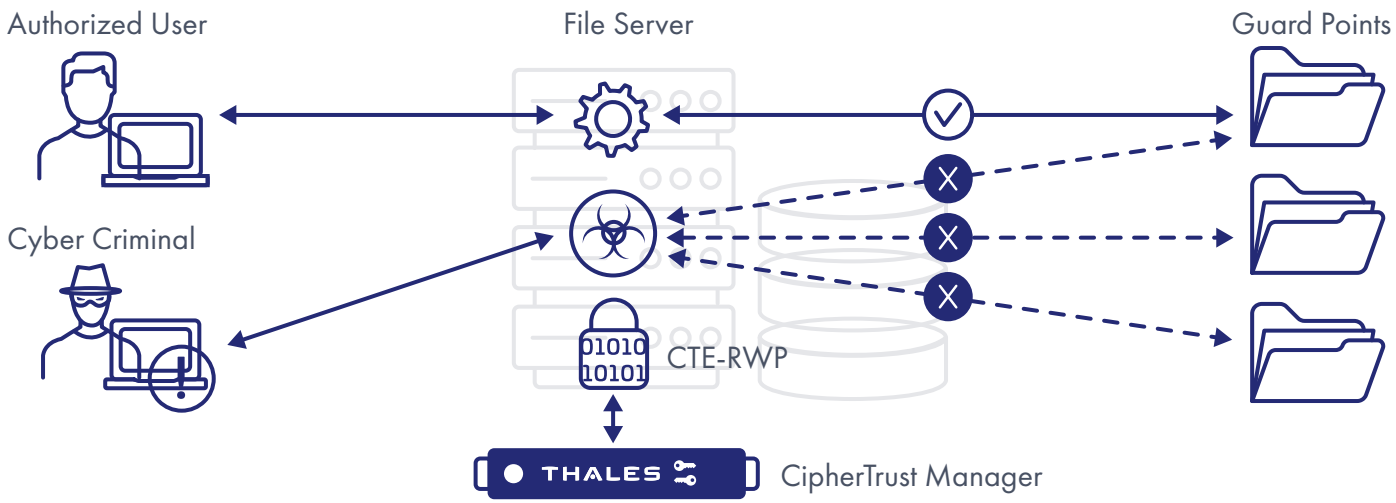
Customers can add Multi-factor Authentication (MFA) for CipherTrust Encryption (CTE), to get an additional layer of protection at the folder/file level. MFA for CTE prompts system administrators and privileged users to demonstrate an additional factor of authentication beyond passwords when they try to access to sensitive data sitting behind Guard Points.

MFA for CTE is available for the Windows platform. It supports integrations with multiple authentication providers including Thales' SafeNet Trusted Access, Okta and Keycloak.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com



CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP)

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com