EXCLUSIVE NETWORKS | THALES
Building a future we can all trust

Challenge

Ransomware Blocks Access to Business-Critical Data

1. Ransomware has been on the rise since 2020. It accounts for 25% of all data breaches. Ransomware attacks can bring business operations to a grinding halt by blocking access to critical data until a ransom is paid.

2. A ransomware attack is expected to strike businesses and individuals every 2 seconds by 2031. 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. The main challenge facing organisations is to safeguard business critical data from being encrypted by unauthorised 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 licence.

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.

Licencing

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

Additional Data Protection Against Ransomware

With CipherTrust Transparent Encryption, customers can maximise ransomware protection on their endpoints/servers, by adding a licence 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 business critical data resides.

•Places strict access control policies around backup processes, including encrypting backups to prevent data exfiltration.

•Guards 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

•Encrypts business critical data, wherever it resides on-premise or in the cloud.

•Makes critical data worthless to intruders, since they cannot monetise encrypted data by threatening to publish.

•Guards 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 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

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organisations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation. Decisive technology for decisive moments.

As well as bringing experience first networking to your partners, we can further enhance the commercial opportunity with Exclusive Networks value added services.

Target Customers

Key Persona Security Teams

• Chief Information Security Officer (CISO)

• Security Practitioner

Role and Responsibilites

• Implementing and overseeing an organisation's cybersecurity program.

• Aligning cybersecurity and business objectives.

• Reporting on cybersecurity.

• Monitoring Incident Response Activities.

Key Persona IT Teams

• Chief Information Officer (CIO)

• Active Directory Administrator (AD Admin)

Role and Responsibilities

• Managing IT staff and developing department goals

• Developing and overseeing the IT budget and planning, deploying and maintaining IT Systems

• Managing the organisation's software development needs

• Developing IT policies, procedures and best practices across the organisation

• Staying up to date on IT trends and emerging technologies

Capabilities Overview

• Application Security

• Cloud Security

• Compliance

• Legacy vs Risk-based VM Comparison

• Ransomware

• IT/OT

• Vulnerability Assessment

• Vulnerability Management

• Zero Trust

How to start a conversion

• Are you concerned about the rise in Ransomware in your business?

• Are you confident you have all the relevant tools in place to mitigate against a ransomware attack?

• Are you adequately protecting business critical data from being encrypted by unauthorised processes and users on endpoints and servers?

Scan the code for more information