cpl.thalesgroup.com

THALES
Building a future we can all trust

Ransomware Attacks and How to Prevent them from Disrupting Your Business

White Paper

Contents

3 **Introduction**

3 **Ransomware is Here to Stay**
4 Examples of Recent Ransomware in the News

4 **Anatomy of a Ransomware Attack**
4 Examples of Recent Ransomware in the News

5 **Baseline Security Practices Fall Short**

5 **Ransomware Detection through Behavior Monitoring**

5 **Blocking Ransomware with Robust Data Access Policies**

6 **CipherTrust Data Security Platform**

7 **CTE Ransomware Protection for Malicious Behavior Detection**

7 **How Does CipherTrust Transparent Encryption Prevent Ransomware Attacks**
8 Access Policy Rules in CipherTrust Transparent Encryption.

9 **Conclusion**

9 **About Thales**

Introduction

Ransomware is a vicious type of malware that cybercriminals use to block companies and individuals from accessing their business-critical files, databases, or entire computer systems, until the victim pays a ransom. It is a form of cyber extortion. In fact, double and triple extortion attacks are occurring more and more where not only is the data encrypted, the data is exfiltrated, and/or used for targeted attacks on customers listed within the stolen data.

Statistica estimates there were 493.33 million ransomware attacks globally in 2022, which means about 16 attacks per second. The estimated total costs to the victim organization is in the range of $300,000 to $2 million per incident. In a study of pentesting projects from Positive Technologies, in 93% of cases, an external attacker can breach an organization's network perimeter and gain access. Given these facts, it only makes sense to implement a multifaceted defense against ransomware to safeguard your business-critical data.

"It is an unfortunate fact of life that ransomware is here to stay and that traditional software-based endpoint protection is not able to protect well against this type of malware," said Stu Sjouwerman, founder and CEO at KnowBe4, a company that specializes in training employees on how to detect and respond to ransomware attacks.

Please continue reading below so that you can learn the anatomy of ransomware attacks and explore defense solutions available in the market today. Security policies in CipherTrust Transparent Encryption enable you to prevent rogue processes and unauthorized users from exfiltrating or encrypting your most sensitive data and thereby protect you from ransomware attacks.

CipherTrust Transparent Encryption is part of the CipherTrust Data Security Platform. The CipherTrust Platform unifies data discovery, data classification, data protection, and provides unprecedented granular access controls, all with centralized key management. The products and solutions available on the CipherTrust Platform mitigate business risks associated with data breaches and ransomware attacks.

Ransomware Attacks are Here to Stay

Most ransomware attacks are perpetrated by sophisticated hacking groups that offer a "ransomware-as-a- service" platform, which helps vetted cybercriminals carry out ransomware attacks with a variety of toolkits, including a "call service" to assist attackers in negotiations and payments from victims.

Even more recently, there have been attempts to create ransomware with the assistance of AI technology such as ChatGPT. A sophisticated cybercriminal, together with AI, could prove a troublesome team. Regardless of how cybercriminals attack, the attacks are becoming more sophisticated and easier to execute. Regrettably, Ransomware attacks are here to stay.

67% of respondents affected by ransomware say they experienced some data loss from the attack.

Examples of Recent Ransomware in the News

Four examples of ransomware attacks reported in April 2023 show that the critical infrastructure of any country can be targeted by sophisticated cybercriminals and nation-states. These recent cyber-attacks have gotten attention at the highest levels of government in the United States, with the White House issuing an Executive Order to improve the nation's cybersecurity.

- A brand owner of fast food chains, sent out data breach notification letters to an undisclosed number of individuals whose personal information was stolen in a January 2023 ransomware attack. As a direct result of the January ransomware attack, the company was forced to shut down hundreds of restaurants for one day in the United Kingdom.
- An American software and technology consulting company, confirmed they suffered an outage on their point of sale platform for hospitality customers after a ransomware attack affected data centers powering their POS platform.
- An American company which designs and manufactures network infrastructure products, was listed on the dark web leak site. Hackers published a trove of data stolen from the U.S. network infrastructure giant, including thousands of employees' Social Security numbers and bank account details.
- A Taiwanese PC vendor revealed that some of its information service systems had been affected by a cyberattack. A ransomware gang claimed to have infiltrated some of the company's systems and stolen files that would be leaked online the following week if the company refused to pay a $4 million ransom.

Anatomy of a Ransomware Attack

This section describes the typical Cyber Kill Chain®, which walks through each of the seven stages of a targeted ransomware attack providing visibility into the intruders' tactics, techniques and procedures (TTPs).

Step 1: Reconnaissance – intruder harvests email addresses of all employees in a company and prepares to launch a phishing campaign.

Step 2: Weaponization – intruder uses a ransomware kit purchased off the dark web tailored to deliver malware through an email attachment.

Step 3: Delivery – intruder delivers the ransomware through a fake email as the payload or through a remote desktop protocol (RDP) service.

Step 4: Exploitation – When an employee unknowingly opens the fake email attachment, the malware exploits a known vulnerability and infects their device.

Step 5: Installation – The ransomware installs as a binary which opens an access point (backdoor) to communicate with a command and control site.

Step 6: Command and Control (CnC) – Ransomware sends target host IP address and gets encryption key needed for encrypting all files and databases.

Step 7: Action – Ransomware exfiltrates sensitive documents to the CnC server, encrypts files and databases then displays a ransom note to the end user.

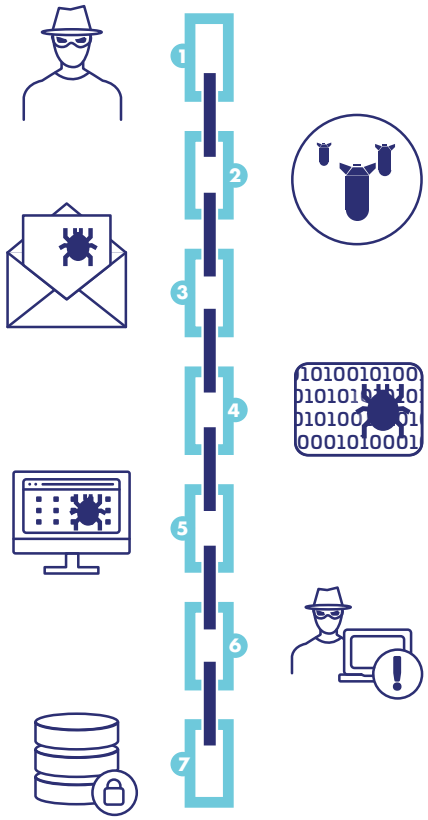


Figure 2: The Seven Stages of the Cyber Kill Chain®

Ransomware Detection Methods

	Detection by signature	Detection by Traffic	Detection by file behavior**
Applied in	**The majority of antivirus software**	**Traffic analystics solutions**	**Some antivirus and data protection software**
Pros	Fast and widely availble	Detects modified ransomeware	Detects modified ransomware
Cons	Inability to detect modified ransomware	High false positive can lock data use	Detection takes some time*

Baseline Security Practices Fall Short

Most organizations follow baseline security practices to prepare for ransomware attacks. However, these practices are not enough to proactively protect business critical data before, during or after a ransomware attack.

- **Security Awareness Training:** Training your employees to recognize suspicious phishing emails through simulation exercises to defend against attack delivery. A good idea, but not enough --it only takes one employee to make the mistake of opening a phishing email to infect their company's network.
- **Deploy Secure Email/Web Gateways:** This technique can be used to defend against ransomware attacks delivered through email. However, security web/email gateways are unable to detect any new strains of malware, because they do not have the file signatures for undiscovered malware
- **Apply the Latest Software Patches:** Regularly scanning all your systems and patching high priority vulnerabilities helps defend against holes exploited by ransomware. However, ransomware can be delivered with day 0 methods, and it is difficult to guarantee 100% patched systems in today's complex environments.
- **Monitor DNS Queries:** After ransomware infects a server/endpoint, the ransomware typically calls a command and control (CnC) sever to exchange encryption keys. Monitoring DNS queries to known ransomware domains (e.g., "killswitch") and resolving them to internal sinkholes can prevent ransomware from encrypting files. However, DNS servers are unable to block unknown CnC domains used by new ransomware attacks.
- **Backup Your Critical Data Regularly:** There still may be times when all your security defenses fall short, and the ransomware attack succeeds in encrypting all your business-critical data. The best way to recover from a ransomware attack is to maintain a secure backup and also have a clear recovery plan that enables you to restore your business-critical data. However, restoration is often expensive and time consuming. In addition, you still need to determine if the malware is still in your system, and you need to identify and close the entry point, otherwise restoration will only be a temporary fix.

Ransomware Detection through Behavior Monitoring

To effectively stop a successful ransomware attack, a multifaceted strategy is highly recommended which would include a behavior monitoring solution in the mix. Ransomware has certain identifiable traits such as encryption and often exfiltration. Sophisticated ransomware will try to hide or obfuscate its intent through various means so behaviors such as file renaming, changing file extensions, deleting file headers and more. Behavior monitoring solutions such as CTE Ransomware Protection monitor the processes for these telling actions in order to detect and block these attacks. Behavior monitoring in the mix helps mitigate risk because it does as follows:

- Enables the detection of zero-day attacks since it monitors for behaviors and doesn't simply look for file signatures of known ransomware stored in an online database.
- Detects ransomware even when disconnected from the internet as it doesn't need connectivity to a database of known ransomware signatures.

- Is able to block ransomware even when the malware infected the system prior to installation of the ransomware monitoring solution.
- Can exclude from monitoring any processes that are added to a trusted processes list.

Blocking Ransomware with Robust Data Access Policies

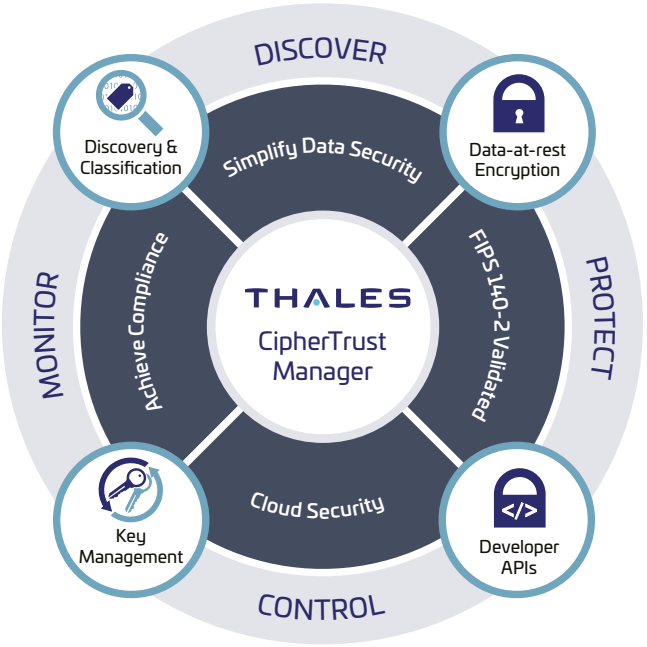
Another layer in an effective ransomware defense to block any unknown malware (ransomware binaries) from taking your data hostage, a robust data security solution that can provide the following capabilities is critical:

- Application Permit-lists that identify "trusted applications" – A "permit list" of files (binaries) that are approved to access protected folders and devices to perform encryption/decryption. The permit also needs to provide a way to check the integrity of trusted applications with signatures to prevent polymorphic malware from getting into approved binaries.
- Apply Fine-grained Access Controls to your business-critical data, which defines who (user/group) has access to specific protected files/folders and what operations (encrypt/decrypt/read/write/directory list/execute) they can perform.
  - Prevent administrative users from exploiting their privileges to gain read access to sensitive files or databases.
  - Place strict access control policies around backup archives, and also encrypt backups to prevent data exfiltration.
  - Implement separation of duties whereby database users are allowed to gain read/write access, while backup software has only read access.
- Data-at-rest Encryption protects data wherever it resides in on-premises data centers or in public/private clouds. This makes the data worthless to intruders when they steal business-sensitive data and threaten to publish it, if the ransom is not paid.

CipherTrust Data Security Platform

CipherTrust Data Security Platform (CDSP) unifies data discovery, classification, data protection and unprecedented access controls with centralized key management - all in a single platform.

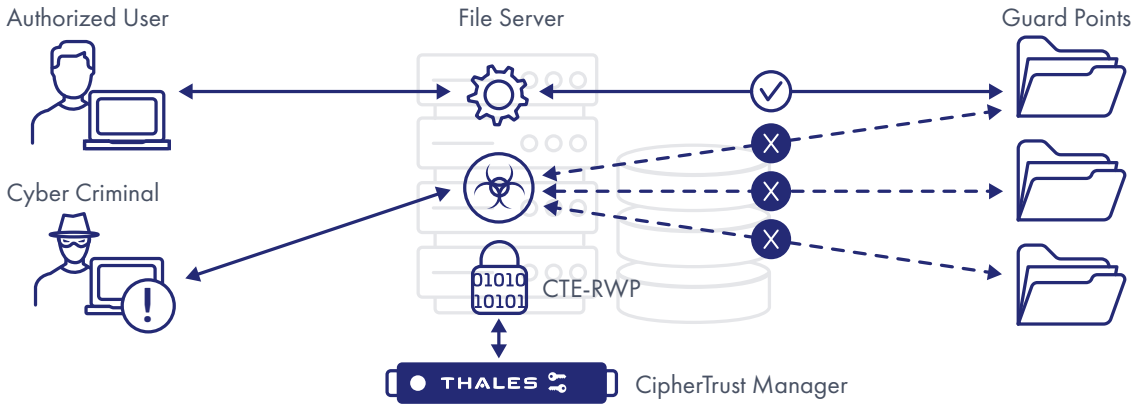
CDSP, also referred to as "the CipherTrust Platform," supports comprehensive data security capabilities, including behavior monitoring for ransomware protection, file-level encryption with access controls, application-layer encryption, database encryption, masking, vaultless tokenization with policy-based dynamic data masking, and vaulted tokenization to support a wide range of data protection use cases. The CipherTrust robust enterprise key management and secrets management work across multiple cloud service providers (CSPs) and hybrid cloud environments to centrally manage encryption keys and secrets, and configure security policies so organizations can discover, protect and control sensitive data in the cloud, on premise and across hybrid environments.



CTE Ransomware Protection (CTE-RWP) for Malicious Behavior Detection

CipherTrust Transparent Encryption Ransomware Protection continuously enforces volume level ransomware protection with minimal configuration and no modification to any applications on the protected volume. CTE-RWP actively monitors processor activity, looking for malicious behaviors caused by ransomware, and sends an alert or blocks the process when malicious behaviors are detected.

Easy to Deploy, CTE-RWP equips administrators to enable ransomware protection without setting up access controls and encryption policies on a per file/folder basis. If exceptions are desired, a "trusted list" can be set up to avoid unwanted monitoring.



CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP)

How CipherTrust Transparent Encryption Prevents Ransomware Attacks

CipherTrust Transparent Encryption (CTE) is one of the most widely-deployed data protection products within the CipherTrust Data Security Platform. CTE provides data-at-rest encryption, fine-grained access control and trusted applications list capabilities, enabling organizations to prevent ransomware attacks. CTE protects both structured and unstructured data with policy-based access controls to files, volumes, databases, containers, and big data wherever it resides whether in the cloud, on premise or across hybrid environments.

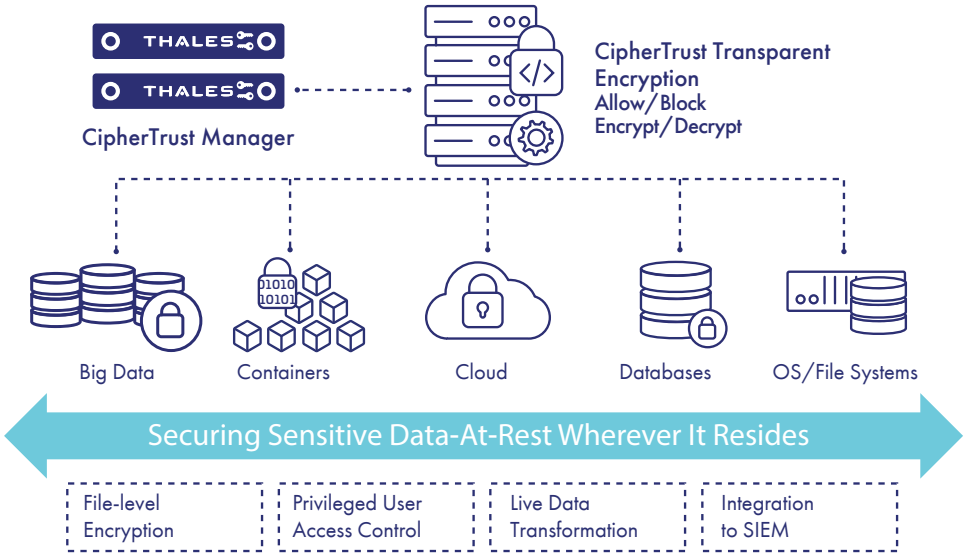


Figure 3: CipherTrust Transparent Encryption

Access policies can be defined to create a trusted applications list to prevent any untrusted binaries (e.g., ransomware) from accessing data stores protected by CTE and to prevent privileged users from accessing user data in files and databases. Access policies enable you to block any rogue binaries from encrypting files/databases/devices, even if the intruder has execute permissions for that binary and read/write permissions to the target file that contains business-critical data. CTE can stop privilege escalation attacks by preventing administrators from reading/writing to protected folders/ files/devices.

Access Policy Rules in CipherTrust Transparent Encryption.

CipherTrust Transparent Encryption uses the concept of "GuardPoints" that are resources protected by access policies. A GuardPoint can encompass a complete disk drive volume, a disk partition, a specific directory or an AWS S3 bucket under which all the unstructured files or structured database files reside. Each access policy is a set of rules that are checked when a file in a protected GuardPoint is being accessed. If the result of the test against the rule is TRUE, the privilege defined in the Effect field is granted, otherwise the test proceeds to the next rule. If none of the rules match, access to the file is denied.

Components of a Rule	Effect
Resource	Specifies which directories in a GuardPoint are being protected by the policy
User Sets	Specifies a set of users/groups who can access the files
Process Sets	Specifies a set of executables that can operate on the file
When	Specifies the time range when the files can be accessed
Action	Specifies the allowed file action – read, write, remove, rename. make directory
Effect	• Permit/Deny: Access to data • Apply Key: Encrypt or decrypt data written to GuardPoint with Key in the KeySelection rule • Create log record every time GuardPoint is accessed

Let us now look at how a customer can protect a Microsoft SQL Server database from a ransomware attack using three simple yet powerful access control policies in CTE with a couple of "set-lists" as shown below.

CipherTrust Transparent Encryption (CTE) access policies to protect the SQL Database folder (aka GuardPoint):

- **Step 1:** Create a privileged User Set-list which includes administrative users.
  - Privileged-Admin-Users: Administrators, Domain Admins
- **Step 2:** Create a process set-list which identifies trusted executables allowed to perform database operations using "signed binaries." A process set-list ensures that only legitimate applications/binaries can access protected resources such as file-systems, disk partitions and cloud object storage.
  - SQL-Processes: File/Folder: c:\Program Files\Microsoft SQL Server\MSSQLSERVER\MSSQL\Binn\
- **Step 3:** Create three access control lists in the SQL-Operational-Policy File. Any user or process that passes a specific rule check during file I/O gets only those permissions listed in action and the privileges listed in the effect field of each ACL.
  - Entry 1: Create a "permit list" of trusted processes that are allowed to access the database for all normal database operations.
    - This Rule will only allow SQL-Processes to encrypt using the key mentioned in the key selection rule below.
    - Rule 1: Process= SQL-Processes; Action= all_ops; Effect= Apply Key, Permit;
  - Entry 2: Prevent hackers from gaining unauthorized access to database contents using privilege escalation
    - This Rule will permit privileged admin users to only read metadata and audit all administrative operations.
    - Rule 2: User= Privileged-Admin-Users; Action= read; Effect= Audit, Permit;
  - Entry 3: Prevent any rogue ransomware binaries from encrypting files underneath the MSSQL database directory.
    - This Rule will deny any users or processes that were not allowed by the 2 Rules above.
    - Rule 3: Default Deny Rule= Effect= Audit, Deny
  - Define the encryption key to be used for encrypting the database, in whichever Rule that has the 'Apply Key" as the privilege (effect).
    - Key Selection rule = Key1

The CTE agent creates detailed actionable audit events that can be sent to SIEM systems to provide unprecedented insight into file access activities allowing you to identify and stop threats before they become full-blown ransomware attacks.

Locking Down Systems

In addition to encryption and a rich set of access controls, CTE also provides a "System Lock" capability which can be optionally deployed to lock down specific system directories and files. Surreptitious alterations or deletions of the designated files and directories is prevented and audit message alerts are sent.

Conclusion

To prepare for a ransomware attack, organizations can employ many different network, endpoint and application security measures. . When an attack is starting, organizations need to respond with a robust data security solution that protects your sensitive data before, during and after an attack. The CipherTrust Data Security Platform (CDSP) can reduce TCO for organizations of all sizes by simplifying data security, accelerating time to compliance, and delivering multi-cloud security and control. Built on an extensible infrastructure, the platform enables your IT and security organizations to discover, classify, and protect data –at rest across your organization in a uniform and repeatable way.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations 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.