Trusted Cyber Technologies

THALES

Prevent Ransomware Attacks from Disrupting Your Agency with the CipherTrust Platform

White Paper

Contents

Introduction

Ransomware is a vicious type of malware that cybercriminals use to block organizations and individuals from accessing their critical files, databases, or entire computer systems, until the victim pays a ransom. It is a form of cyber extortion.

Cybersecurity Ventures predicts that a organization will fall victim to a ransomware attack every 11 seconds, and the estimated cost to organizations globally will be around $20 billion by 2021. The direct costs can be attributed to the ransom demands -- if the victim chooses to the pay the ransom -- while the indirect costs are associated with the downtime, data recovery, lost revenue, improvements to cyber defenses, and reputational damage to the organization.

"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.

This white paper helps you understand the anatomy of ransomware attacks and explores the solutions available in the market today to defend against such attacks. It illustrates how security policies in CipherTrust Transparent Encryption from Thales Trusted Cyber Technologies (TCT) enable you to prevent rogue processes and unauthorized users from exfiltraing or encrypting your most sensitive data and thereby protects you from ransomware attacks. CipherTrust Transparent Encryption is part of the CipherTrust Data Security Platform. The CipherTrust Platform unifies data discovery, classification, data protection, and provides unprecedented granular access controls, all with centralized key management. The products and solutions available on the CipherTrust Platform mitigate the organization risks associated with data breaches and ransomware attacks.

Ransomware on the Rise

The Internet Crime Compliant Center (IC3), a branch of the FBI that provides the public a trustworthy source of information on all cybercriminal activity in the US, received a record 2,474 ransomware incidents in 2020, which is a 60% increase over the number of attacks in 2018. As United States is emerging out of Cornonavirus lock downs, it is combating a different kind of pandemic, as former head of cybersecurity Chris Krebs warned in May 2021.

Cybersecurity Ventures predicts that all types of organizations will fall victim to ransomware attacks every 11 seconds, and the estimated cost globally will be around $20 billion by 2021.

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

> **" A business will fall victim to a ransomware attack every 11 seconds by 2021, and the estimated cost to all businesses put together will be around $20 billion"**
>
> **– Cybersecurity Ventures**

Examples of Recent Ransomware in the News

Here are three examples of recent ransomware attacks, which show that the critical infrastructure of any country can be targeted by sophisticated cyber criminals and nation-states. These recent cyber attacks has gotten the attention at the highest levels in the United States, with the White House issuing and Executive Order on improving the nation's cybersecurity.

- JBS USA, the world's largest meat processing company, was hit by massive ransomware attack in June 2021. It temporarily shutdown operations in Australia, Canada, and the US, leading to meat shortages and raising prices for consumers.
- The Colonial Pipeline ransomware attack in May 2021, resulted in a weeklong shutdown of the 5500-mile long pipeline, leading to fuel shortages, a spike in fuel prices, and creating panic at gas stations across the US east coast.
- Europe's largest private hospital chain operated by Fresenius Group was hit by the Snake ransomware attack. They are a major provider of kidney dialysis machines and services to the largest hospitals across Europe and United States, which are in high demand during the Covid-19 pandemic. The intruders were holding their IT systems and data hostage in exchange for payment in a digital currency, such as bitcoin.

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. It provides visibility into the intruders' tactics, techniques, and procedures (TTPs).

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

Step 2: Weaponization – intruder uses a ransomware kit purchased off the dark web tailored to deliver that 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 laptop.

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 and then encrypts those files and databases. It then displays a ransom note to the end user.

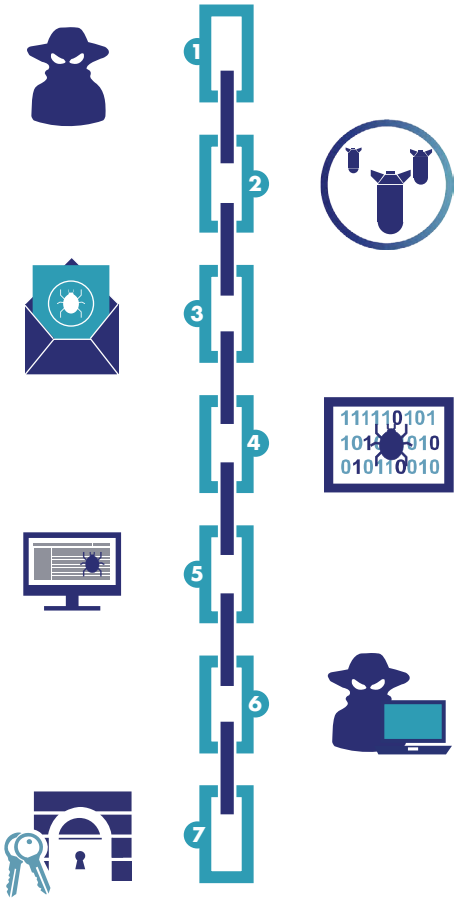


Figure 2: The Seven Stages of the Cyber Kill Chain®

Baseline Security Practices Fall Short

Most organizations follow these baseline security practices to prepare for ransomware attacks. However, these practices are not enough to proactively protect their organization 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. However, it only takes one employee to make the mistake of opening a phishing email and infecting their organization'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 a new strain of malware, because they do not have the malware signature.
- **Apply the Latest Software Patches:** Regularly scanning all your systems and patching high priority vulnerabilities helps defend against holes exploited by a 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 a ransomware infects a server/endpoint, it 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 organization 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 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.

Blocking Ransomware with Robust Data Access Policies

In spite of all the investments organizations make in traditional perimeter and endpoint security technologies, data breaches and ransomware attacks continue to make headlines.

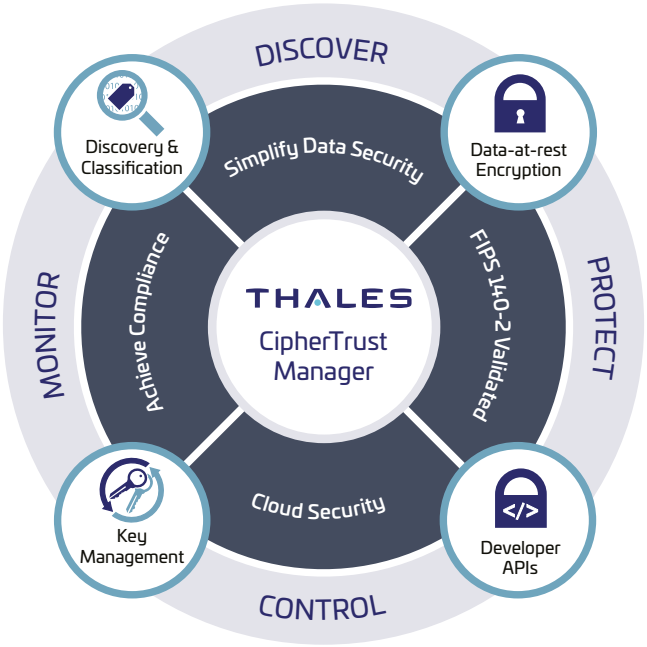
To effectively block any unknown malware (ransomware binaries) from taking your data hostage, security organizations need a robust data security solution that can provide the following capabilities:

- **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. It also needs to provide a way to check the integrity of these applications with signatures to prevent polymorphic malware from getting into approved binaries.
- **Apply Fine-grained Access Controls** to your 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 such that, database users are allowed to gain read/write access, whereas backup software has only read access to the same database.
- **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 organization sensitive data and threaten to publish it, if the ransom is not paid. In addition, some ransomware selectively encrypts files so that it doesn't take systems entirely offline. Others look for sensitive data and only encrypt those files. In this case, encrypted files aren't accessible to the malware and hence not attacked.

CipherTrust Data Security Platform

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

The CipherTrust Platform provides comprehensive data security capabilities, including 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. It delivers robust enterprise key management across multiple cloud service providers (CSP) and hybrid cloud environments to centrally manage encryption keys and configure security policies so organizations can discover, control and protect sensitive data in the cloud, on-premise and across hybrid environments.



How CipherTrust Transparent Encryption Prevents Ransomware Attacks

CipherTrust Transparent Encryption is one of the widely deployed data protection products within the CipherTrust Data Security Platform. It provides data-at-rest encryption, fine-grained access control and application whitelisting capabilities, enabling organizations to prevent ransomware attacks. It protects both structured and unstructured data with policy-based access controls to files, volumes, databases, containers, and big-data wherever it resides on-premises and in hybrid cloud environments.

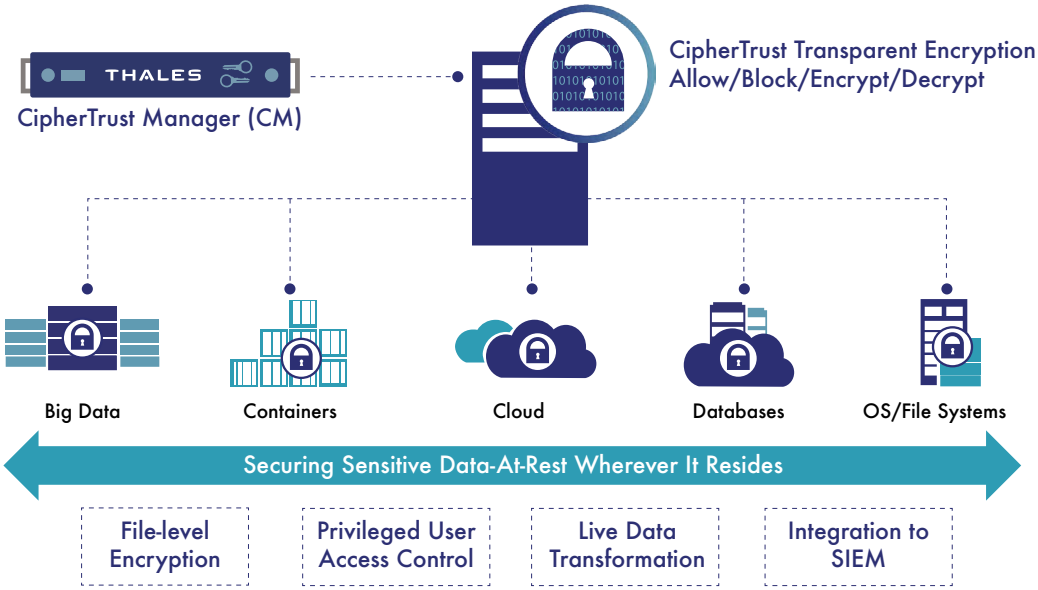


Figure 3: CipherTrust Transparent Encryption

Access policies can be defined to create a whitelist of "trusted" applications to prevent any untrusted binaries (e.g. ransomware) from accessing data stores protected by CipherTrust Transparent Encryption and to prevent privileged users from accessing user data in files and databases. These 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 critical data. CipherTrust Transparent Encryption 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, 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 is 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 CipherTrust Transparent Encryption with a couple of "set-lists" as shown below.

CipherTrust Transparent Encryption 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". This 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 privileges 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 from only reading meta data 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

CipherTrust Transparent Encryption 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 faster and to proactively alert you to ransomware attacks before they happen, improve visibility, and streamline regulatory compliance.

Locking Down Systems

In addition to encryption and a rich set of access controls, CipherTrust Transparent Encryption also provides a "System Lock" capability, which can be optionally deployed to lock down specific system directories and files. Surreptitious alterations or deletions of these files and directories are prevented along with audit message alerts.

Conclusion

There are many different network, endpoint and application security measures that organizations can take to prepare for a ransomware attack. However, they do not proactively protect your critical data. Deploying a robust data security solution can protect your sensitive data before, during and after a ransomware attack. The CipherTrust Data Security Platform 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 rusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

> 3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070

• info@thalestct.com thalestct.com