cpl.thalesgroup.com

THALES

Prevent Ransomware Attacks from Disrupting Your Business with CipherTrust Data Security Platform

White Paper

Contents

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.

Cybersecurity Ventures predicts that a business will fall victim to a ransomware attack every 11 seconds, and the estimated cost to businesses 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 company.

"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.

> " 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

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 enable you to prevent rogue processes and unauthorized users from 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 business risks associated with data breaches and ransomware attacks.

Ransomware on the Rise

While the frequency of ransomware attacks has fluctuated over the years, 2019 saw a 41% increase over the previous year. Ransomware campaigns have evolved from high-volume "spray-and-pray" attacks that target small businesses and home users to low-volume "big game hunting (BGH)" attacks that target medium to large businesses that have the funds or insurance coverage to pay large ransoms.

According to CrowdStrike®, an endpoint security vendor, established criminal organizations have started offering Ransomware-as-a-Service (RaaS) to weaponize ransomware kits and make it easier for less sophisticated cyber criminals to launch such attacks and make fast money.

Here are some alarming statistics to consider regarding whether your company could be the next target of ransomware attacks.

During 2019 in the U.S. ransomware infected...

Figure 1: Ransomware Statistics in the United States for 2019

- Nearly 1000 US organizations were impacted by ransomware attacks in 2019 as shown in Fig. 1 above, according to Emsisoft.
- The average downtime for companies to recover from ransomware infections was 16.2 days in 2019, according to Coveware.
- The average ransomware payment increased to $84,116 in Q4 2019, according to Coveware.
- 25% of the ransomware incidents in Q3 2019 involved IT vendor or MSP compromises, according to insurance provider Beezley.

Examples of Recent Ransomware in the News

There has been a considerable increase in ransomware attacks in the news lately.

- 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.
- The Sodinokibi group allegedly hacked into Grubman Shire Meiselas & Sacks (GSMLaw), based in New York, using Sodin and REvil ransomware. They not only encrypted all the legal documents of the law-firm but also threatened to release sensitive data that included contracts, phone numbers, personal correspondence, and non-disclosure agreements of their big-name clients (such as Robert DeNiro, Lady Gaga, Elton John, and many more), if ransom was not paid.
- Australia's logistics giant Toll Group suffered a second ransomware attack within three months. A new strain of ransomware known as Nefilim gained privileged access using a brute-force password attack to systems that were running remote desktop protocol (RDP) services. The intruders demanded a double-extortion by not only encrypting the users' files but also threatened to publish the data online through name and shame tactics.

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 company 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.

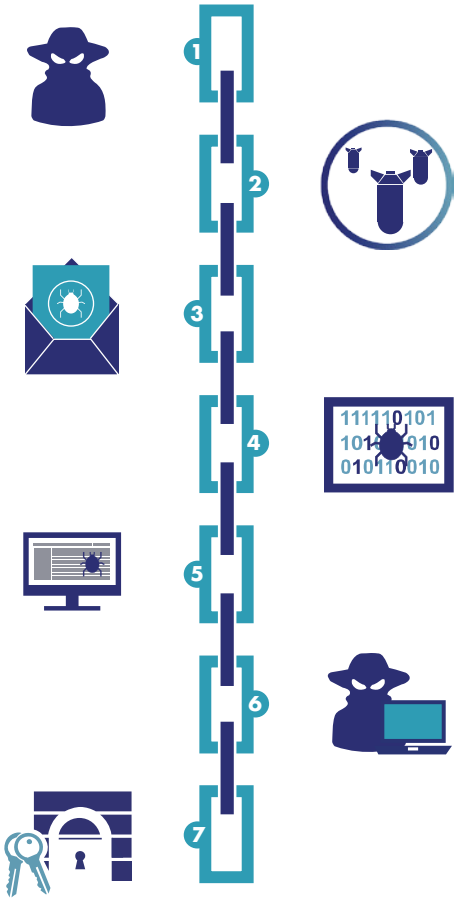


Figure 2: The Seven Stages of the Cyber Kill Chain®

Baseline Security Practices Fall Short

Most organizations follow baseline security best practices listed below, when defending against ransomware attacks. However, they come up short in most cases.

- **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 his 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 a new strain of malware, because it does not have the 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 any 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 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 companies make in traditional perimeter and endpoint security technologies, data breaches and ransomware attacks continue to make headlines.

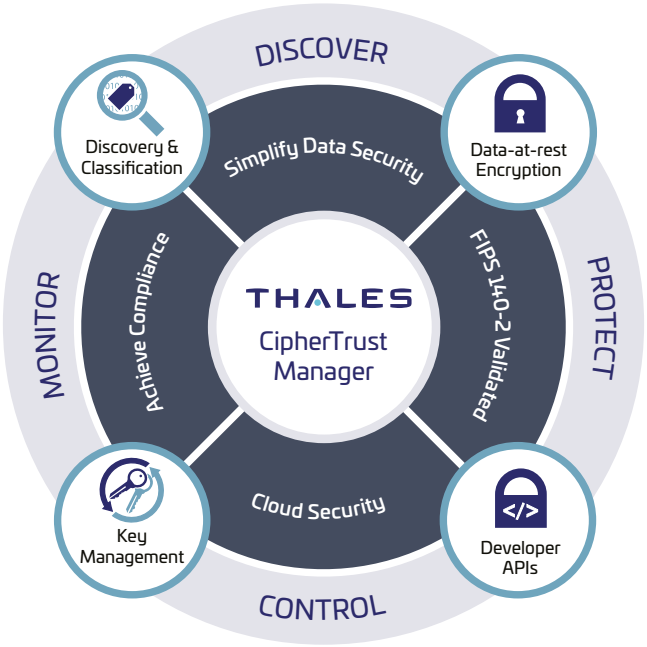
To effectively block any unknown malware (ransomware binaries) from taking your data hostage, security organizations need a robust data security solution that can provide the following capabilities:

- **Application Whitelisting that identifies "trusted applications"** – binaries which are approved to perform encryption/decryption of business critical files. 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 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. Some malware depends on escalating privileges to gain system access. Appropriate access control solutions can bar privileged users from examining and even accessing resources.
- **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. 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 scanned by the malware and hence not attacked.

CipherTrust Data Security Platform

CipherTrust Data Security Platform from Thales, 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 Does CipherTrust Transparent Encryption Prevent 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, big-data wherever it resides on-premises and in hybrid cloud environments.

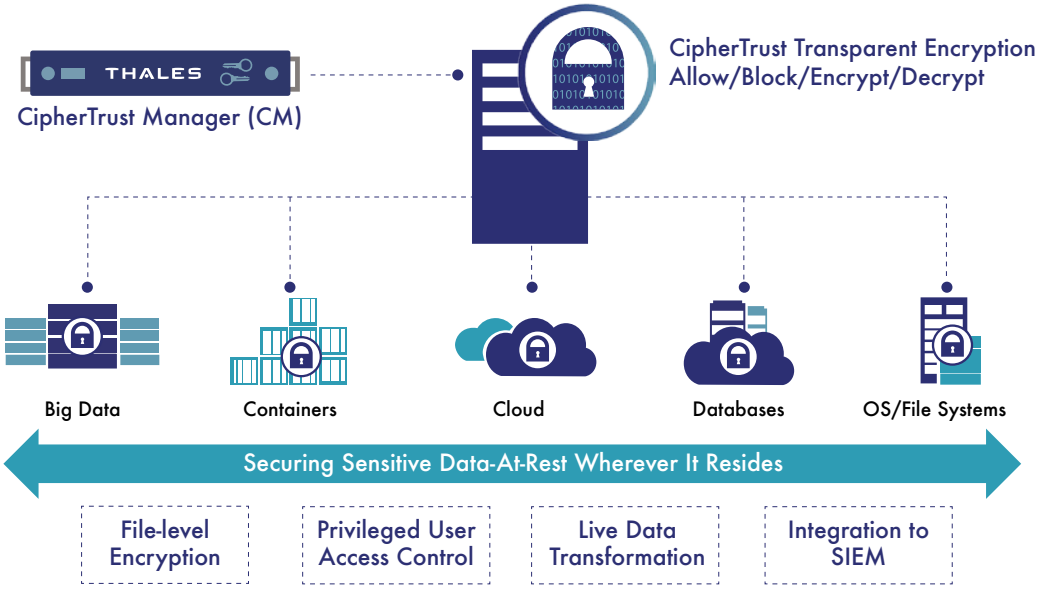


Figure 3: CipherTrust Transparent Encryption

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 can enable you to block any rogue binaries from encrypting files/databases, even if the intruder has execute permissions for that binary and read/write permission to the target file that contains business critical data.

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 specific directory or an AWS S3 bucket under which all the unstructured files or structured database files reside. Each access policy is an access control list (ACL) entry, that includes the following five criteria (shown in Table 1) that are checked when a protected GuardPoint is being accessed. If the result of the ACL test is TRUE, then the privilege defined in the Effect field is granted, otherwise the test proceeds to the next ACL, similar to firewall ACLs.

Criteria	Action
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 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 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 includes trusted executables for database operations with the signature of each process that is checked at the time of execution
  - SQL-Processes: <signature>; 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 ACL 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 "whitelist" of trusted processes that are allowed to access the database for all normal database operations.
    - This ACL will only allow SQL-Processes to encrypt using the key mentioned in the key selection rule below.
    - ACL 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 ACL will permit privileged admin users from only reading meta data and audit all administrative operations.
    - ACL 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 ACL will deny any users or processes that were not allowed by the 2 ACLs above.
    - ACL 3: Default Deny Rule= Effect= Audit, Deny
  - Define the encryption key to be used for encrypting the database, in whichever ACL 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.

Conclusion

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. Using a legacy approach can often require expensive, dedicated point products which may require further integration and additional staff time to manage, negating any potential cost savings. The many products available on the CipherTrust Data Security Platform can be deployed individually or in combination, and they prepare your organization for the next security challenge or compliance requirement at the lowest TCO. By integrating data discovery, classification, risk analysis, data protection, and reporting into a single platform, the CipherTrust solution frees IT staff and budget for more strategic tasks and empowers the openness and freedom of collaboration the modern organization needs–without sacrificing security.

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.