Thales Accelerate
Partner Network

Prevent Ransomware Attacks with Thales Solutions

Partner Campaign in a Box

June 2023

Partner use only, not for customer distribution

THALES
Building a future we can all trust

How to use this Campaign in a Box?

Campaign Overview

Ransomware attacks have become a top cybersecurity concern, with criminals targeting everything from critical infrastructure to hospitals and retailers, and demanding tens of millions of dollars in ransom. Unfortunately, ransomware is a complex cybersecurity problem with no silver bullet to address this menace.

Thankfully the National Institute of Standards and Technology (NIST) released guidance on identifying and protecting assets against ransomware. The Cybersecurity Special Publication (SP) 1800-25 lays out the steps to having a comprehensive strategy around protecting assets.

Thales provides organizations with data security and access management solutions to mitigate ransomware attacks.

Campaign Aim

The aim of the campaign is to both attract new, and nurture existing customers by promoting Thales as the worldwide leader in data and software protection.

To help accelerate your conversations with customers, we have provided partners with a collection of pre-written e-mails and social posts, highlighting our most valuable sales and marketing campaign resources.

This easy-to-use guide puts the available sales and marketing assets, as well as tips for supporting your sales efforts – all in one place.

Prevent Ransomware Attacks with Thales Solutions

Ransomware Prevention

- Thales data security and access management solutions provide some of the most essential components of the cybersecurity framework to protect organizations against ransomware.

- **Thales' industry-leading portfolio provides organizations the ability to:**

- Discover sensitive data and classify it according to risk

- Implement robust identity and access management control

- Protect and control sensitive data at rest and in transit through encryption and tokenization

- Monitor data security for intelligent remediation

Thales Solutions

- Safeguard data-at-rest from ransomware attacks with the CipherTrust Data Security Platform

- Implement strong authentication, access and identity management with SafeNet Trusted Access

- Identify and classify vulnerable sensitive data across hybrid IT with CipherTrust Data Discovery and Classification

- Protect data in transit with Thales High Speed Encryptors and secure data-in-motion

Value Proposition for new and existing customers

Thales offers access management and data protection solutions that can prevent unauthorized users from gaining access to an organization's systems, escalate privileges and encrypt all sensitive data using malware.

Multifaceted Ransomware Defense with CipherTrust Transparent Encryption

- Thales CipherTrust Transparent Encryption of data, user access policies, key management, and MFA are all part of data fortification
- CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) is a specific protection that monitors for ransomware type activities to stop the malicious processes

Implement Strong Authentication, Access and Identity Management

- Thales SafeNet Trusted Access offers multi-factor authentication at all login entry points protecting enterprise IT, web, and cloud-based applications from internal and external threats at the front door
- STA utilizes policy-based conditional access, rigorous single sign-on (SSO), multi-factor authentication (MFA), and universal authentication methods, which prevent breaches, simplifies regulatory compliance and enables enterprises to migrate securely to the cloud

Protect Data In Transit with Thales High Speed Encryptors

- Thales Network Encryption solutions provide customers with a single platform to encrypt everywhere
- High Speed Encryptors offer the ideal certified and proven solution for data-in-motion security, including time-sensitive voice and video streams, for enterprise, and government organizations

Campaign Objectives and Messaging

Campaign Objectives

- Enable partners to build more pipeline, opportunities and revenue.

- Drive new customers through the sales journey faster by empowering organizations to simplify the discovery, protection and control over their most sensitive data anywhere.

- Remind the market that Thales is global leader in data protection, access management and authentication.

Campaign Messaging

- Thales is a global leader in data protection, access management, and authentication. We help the world's most trusted organizations simplify security for the cloud, achieve regulatory compliance, and reduce risk

- Protect your organization and data against ransomware with Thales

- How to build a comprehensive strategy against ransomware with Thales

- Stop ransomware in its tracks with strong data security

- Ransomware Protection: how to keep your data safe with strong data security

How to use the campaign for lead generation

Build your own e-mail marketing campaign

- Use the campaign messaging provided to build your own e-mail campaign track <u>OR</u>
- Build your campaign quickly and easily using the NEW <u>Accelerate Campaigns Center</u> pre written e-mails <u>HERE</u>
- Leverage the <u>Additional Marketing Tools</u> as 'conversation openers' for your sales teams to use
- Suggested campaign flow with the following steps:

① ② ③ ④ ⑤ ⑥ ⑦ ⑧

<u>E-mail #1</u> <u>Social Post</u> <u>E-mail #2</u> <u>Social Post</u> <u>E-mail #3</u> <u>Social Post</u> <u>E-mail #4</u> <u>Social Post</u>

E-mail #1 suggested content for you to use

Subject line and Headline

- Protect your organization and data against ransomware

- Is your data protection holding up against ransomware?

Main copy

- According to the 2023 Thales Data Threat Report, 49% of IT professionals reported an increase in ransomware attacks with 22% of organizations having experienced a ransomware attack in past 12 months.

- Ransomware attacks can bring business operations to a grinding halt by blocking access to critical data until the attack is resolved – a major threat to organizations concerning cost and reputation. In addition to existing perimeter controls, a data-centric approach is needed to safeguard critical data from being encrypted by unauthorized processes.

Call to action

- Find out how you can protect your organization and data against ransomware in this new infographic.

- Or read one of the informative blog posts on the subject:

- The Pain of Double Extortion Ransomware

- Ransomware – To Pay, or Not to Pay?

- How Can You Protect Critical Infrastructure from Ransomware Attacks

Campaign asset

- Infographic: Addressing the growing threat of ransomware

- The Pain of Double Extortion Ransomware

- Blog: Ransomware – To Pay, or Not to Pay?

- Blog: How Can You Protect Critical Infrastructure from Ransomware Attacks

How to use this Campaign

Product Messaging

Value Proposition

Objectives and Messaging

Lead Generation

Suggested Campaign Content

Content for Distributors

Additional Marketing Tools

Contact Us

Social Post - suggested content for you to use

Subject line and Headline

- 51% of organizations do not have a formal ransomware plan – are you one of them?

Main copy

- The latest 2023 Thales Data Threat Report, revealed that 51% of organizations do not have a formal ransomware plan.

- The report also highlights human error as a primary cause of data breaches, the growing importance of digital sovereignty, and the challenges faced in securing multicloud environments.

Call to action

- Check out the latest data security threats and trends in this webinar.

- If you have any questions or would like to find out more, please do not hesitate to contact us via **<insert partner contact information>**.

Social post asset

- Webinar: Key Findings from the 2023 Thales Data Threat Report

E-mail #2 suggested content for you to use

Subject line and Headline

- How to build a comprehensive strategy against ransomware
- How you can prevent ransomware attacks

Main copy

- Cybersecurity standards have always been key to enhance security and reduce risk by providing third party validation and best practices.
- The recently released guidance from NIST* on identifying and protecting assets against ransomware, Cybersecurity Special Publication (SP) 1800-25, lays out the steps for having a comprehensive strategy around protecting assets.
- * United States National Institute of Standards and Technology
- Thales data security, access management and authentication solutions provide some of the most essential components of the NIST cybersecurity framework proposed to protect organizations against ransomware.

Main copy continued

- Thales' industry-leading portfolio provides organizations with the ability to:
- Discover sensitive data and classify it according to risk
- Implement robust access management and authentication
- Protect and control sensitive data at rest and in transit through encryption and tokenization
- Monitor data security for intelligent remediation

Call to action

- Download this new Solution Brief mapping Thales solutions to the NIST cybersecurity framework and ransomware guidance.

Campaign asset

- Solution Brief: Thales Solutions for Ransomware Attack Prevention

Social Post - suggested content for you to use

Subject line and Headline

- How Ransomware attacks leverage unprotected RDPs and what you can do about it

Main copy

- Ransomware attacks targeting enterprises in a variety of sectors have skyrocketed over the past two years. Criminals are taking advantage of our reliance on digital communications and remote working for sinister purposes.

- As a result, most of the ransomware incidents can be attributed to a limited number of intrusion vectors, with the top three being badly secured remote desktop protocol (RDP) endpoints, email phishing, and the exploitation of zero-day VPN vulnerabilities.

Call to action

- Discover how Thales solutions can help you protect your business environment against RDP-based ransomware attacks. Check out this Solution Brief.

Social post asset

- Solution Brief: How Ransomware attacks leverage unprotected RDPs and what you can do about it

E-mail #3 suggested content for you to use

Subject line and Headline

- Discover Thales CipherTrust Transparent Encryption Ransomware Protection

- Monitor and block ransomware behavior to protect critical data

Main copy

- **Effective ransomware defense requires a multifaceted approach**

- Reliance on baseline security practices using 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 Fortune 500 companies is to safeguard business critical data from being encrypted by unauthorized processes and users on endpoints and servers.

- **Stop ransomware in its tracks**

- CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) continuously monitors processes for abnormal I/O activity and alerts or blocks malicious activity before ransomware can take complete hold of your endpoints and servers.

Main copy continued

- Using CTE-RWP as part of your ransomware defense strategy to protect critical data strengthens your overall security posture and avoids business disruption.

Call to action

- Read this Product Brief and discover how CipherTrust Transparent Encryption Ransomware Protection can help your business.

- If you have any questions or would like to find out more, please do not hesitate to contact us via **<insert partner contact information>**.

Campaign asset

- Product Brief: CipherTrust Transparent Encryption Ransomware Protection

Social Post - suggested content for you to use

Subject line and Headline

- Is it easier for cyber criminals to break stuff than it is for us to build it?

Main copy

- Cybercriminals continue to succeed in discovering flaws and weaknesses in every connected technology. From zero days to SQL injection, what most people see as technology designed to perform a specific task, they see as a door, a window, or even a simple crack through which they can gain access.

- Join Amanda Widdowson, Head of Human Factors Capability at Thales UK, and Freaky Clown, the co-CEO and Co-Founder, Head of Ethical Hacking at Cygenta about what makes the criminal mind so good at thinking outside the box, and more importantly, how we can develop those skills inside security professionals, senior managers, and everyday people.

Call to action

- Check out this exciting podcast now.

Social post asset

- Podcast: The Eternal Sunshine of the Criminal Mind

Sidebar navigation

- How to use this Campaign
- Product Messaging
- Value Proposition
- Objectives and Messaging
- Lead Generation
- Suggested Campaign Content
- Content for Distributors
- Additional Marketing Tools
- Contact Us

E-mail #4 suggested content for you to use

Subject line and Headline

- Safeguard your critical data with Thales CipherTrust Transparent Encryption Ransomware Protection

Main copy

- According to the 2023 Thales Data Threat Report, 49% of IT professionals reported an increase in ransomware attacks with 22% of organizations having experienced a ransomware attack in past 12 months.

- Did you know that Thales CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) safeguards your sensitive data from malicious ransomware attacks?

- **Why You'll Love CTE-RWP**

- **Active Detection**: CTE-RWP doesn't rely on known ransomware file signatures. Instead, it monitors active processes to detect ransomware – identifying activities such as excessive data access, exfiltration, unauthorized encryption, or malicious impersonation of a user

- **Easy to manage**: Quickly deploy CTE-RWP as there is no need to configure user access policies. Leverage the same CipherTrust Manager console used for other tools in the CipherTrust Data Security Platform to simplify and unify your data security management

Main copy continued

- **Reliable remediation**: Since CTE Ransomware Protection monitors the processes for identifying activities, it will still flag/block the ransomware activity even if the ransomware was installed on the machine first and went undetected

Call to action

- **Get Started!**

- Find out how CTE Ransomware Protection can help your business.

- Connect with a **<insert partner name>** data security expert for help tailoring a ransomware protection plan to your needs.

- You can also watch a CTE-RWP demonstration here!

Campaign asset

- Video: CipherTrust Transparent Encryption Ransomware Protection Demo

- Don't forget to include your own customer lead capture form and your organization contact information

How to use this Campaign

Product Messaging

Value Proposition

Objectives and Messaging

Lead Generation

Suggested Campaign Content

Content for Distributors

Additional Marketing Tools

Contact Us

Social Post - suggested content for you to use

Subject line and Headline

- Stop Ransomware Attacks in their Tracks with Thales Solutions

Main copy

- Thales has launched CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) to help customers safeguard critical files and folders from ransomware attacks.

- CTE-RWP provides customers with early detection of rogue processes and a non-intrusive way of protecting files/folders from ransomware attacks with minimal configuration.

Call to action

- Discover how to stop ransomware attacks in their tracks with Thales solutions. Read this Blog and learn more.

- If you have any questions or would like to find out more, please do not hesitate to contact us via **<insert partner contact information>.**

Social post asset

- Blog: Ransomware – Stop'em Before They Wreak Havoc

Content for Distributors

Promote this campaign in your newsletter to your partner community

Subject line and Headline

- Help your customers build a comprehensive strategy against ransomware

Main copy

- When it comes to ransomware, traditional security measures are not working anymore. Even when next generation firewalls, email/web security gateways, endpoint detection and response products have been deployed, companies are still suffering from ransomware attacks. Adding robust data security to the network and endpoint security measures will strengthen an organization's defense. **<insert distributor name>** and Thales can help organizations prevent ransomware attacks with a comprehensive set of data security products.

- The Thales industry-leading portfolio provides organizations with the ability to:

- Discover sensitive data and classify it according to risk

- Implement robust access management and authentication

- Protect and control sensitive data at rest and in transit through encryption and tokenization

- Monitor data security for intelligent remediation

- For all our partners, this brings extra value to your sales efforts – whether this be supporting your customers with creating a robust strategy against ransomware, or meeting compliance mandates – your customers can rely on **<insert distributor name>** and Thales to help protect and secure access to their most sensitive information and software wherever it is created, shared or stored.

- Contact your Account Manager today to learn more.

Content for Distributors - promoting to your partners via e-mail

Subject line and Headline

- Help your customers build a comprehensive strategy against ransomware with **<insert distributor name>** and Thales

Main copy

- When it comes to ransomware, traditional security measures are not working anymore. Even when next generation firewalls, email/web security gateways, endpoint detection and response products have been deployed, companies are still suffering from ransomware attacks. Adding robust data security to the network and endpoint security measures will strengthen an organization's defense.

- How can **<insert distributor name>** and Thales help prevent ransomware attacks?

- CipherTrust Data Security Platform offers multiple data security solutions, that help customers discover, protect and monitor business-critical data

- CipherTrust Transparent Encryption Ransomware Protection solution provides a great start for businesses to implement a robust ransomware detection and protection strategy

- SafeNet Trusted Access enforces access management at the login entry points protecting exposed RDPs and VPNs. It utilizes policy-based conditional access, rigorous single sign-on (SSO), and universal authentication methods which prevent malicious actors from accessing networks in order to embed ransomware malware

Call to action

- Support your customers with building a robust ransomware strategy with **<insert distributor name>** and Thales.

- Contact your Account Manager today to learn more.

Additional marketing tools you can use

Briefs

- Product Brief: CipherTrust Transparent Encryption Ransomware Protection

- Product Brief: CipherTrust Data Security Platform

- Product Brief: CipherTrust Transparent Encryption

- Product Brief: Cloud-based Access Management - SafeNet Trusted Access

- Product Brief: Thales CipherTrust Data Discovery and Classification

- Solution Brief: High Speed Encryption Solutions

- Solution Brief: Strengthen your defense against ransomware attacks with privileged access controls for your encrypted data

- Solution Brief: Thales Solutions for Ransomware Attack Prevention

- Solution Brief: How Ransomware attacks leverage unprotected RDPs and what you can do about it

Customer Presentation

- CipherTrust Transparent Encryption Ransomware Protection

Videos

- CipherTrust Transparent Encryption Ransomware Protection Demo

- Leveraging SafeNet Trusted Access and CipherTrust Transparent Encryption to Prevent Ransomware

Infographics

- Addressing the Growing Threat of Ransomware

- How Ransomware uses unprotected Remote Desktop Protocols

Blogs:

- What Are the Key Trends in Cybersecurity Right Now?

- Ransomware – Stop'em Before They Wreak Havoc

- The Pain of Double Extortion Ransomware

- Blog: Ransomware – To Pay, or Not to Pay?

- Blog: How Can You Protect Critical Infrastructure from Ransomware Attacks

White Papers + Reports

- Report: The Total Economic Impact™ Of Thales CipherTrust Data Security Platform

- Report: 2023 Thales Data Threat Report – Global Edition

- **Partners must gate this content for lead generation**

Questions & Special Requests

We are happy to help

Please contact us with any questions:

DLAccelerate.Campaigns@thalesgroup.com