Trusted Cyber Technologies

THALES
Building a future we can all trust

Thales TCT Solutions for Ransomware Attack Prevention

Mapping Thales TCT Solutions to NIST Cybersecurity Framework and Ransomware Prevention Guidance

Ransomware attacks have been a problem for years, but they have recently become a lot more damaging, with criminals targeting everything from critical infrastructure to hospitals and retailers, and demanding tens of millions of dollars in ransom. Today, with global leaders discussing these attacks at high-profile summits, government agencies are taking an active role in educating and providing resources for enterprises and organizations to protect themselves from attacks.

NIST Guidance for Preventing Ransomware Attacks

The National Cybersecurity Center of Excellence (NCCoE) under the auspices of 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. It also shows that there is no silver bullet to address the menace of ransomware.

Thales TCT Solutions for Ransomware Prevention

Thales Trusted Cyber Technologies (TCT) data security and access management solutions provide some of the most essential components of the cybersecurity framework proposed by NIST 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 ransowmare prevention and intelligent remediation

Following is an outline of how our solutions map to the NIST Cybersecurity Framework and ransomware guidance:

Mapping Thales TCT Solutions to NIST Cybersecurity Framework and Ransomware Guidance

Category	Requirement	Thales TCT Solutions
IDENTIFY **Risk Assessment (ID.RA**	ID.RA-1: Asset vulnerabilities are identified and documented.	**CipherTrust Data Discovery and Classification** locates regulated sensitive data, both structured and unstructured, across the cloud, big data, and traditional data stores. A single pane of glass delivers understanding of sensitive data and its vulnerabilities, enabling better decisions about closing security gaps, prioritizing remediation actions, and securing your cloud transformation and third-party data sharing.
PROTECT **Access Control (PR. AC)**	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. PR.AC-3: Remote access is managed. PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**SafeNet Trusted Access delivers Centralized Access Management** that enables organizations to pursue consistent authentication policies across platforms by automating and simplifying the deployment and management of a distributed estate of tokens, while securing a broad spectrum of resources, whether on-premises, cloud-based, or virtualized. **SafeNet Trusted Access also provides Commercial off-the-Shelf Multi-factor Authentication** with the broadest range of authentication methods and form factors. This allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally-managed policies—managed from one authentication back end delivered in the cloud or on-premises. **CipherTrust Transparent Encryption provides Fine-grained Access Controls** to your mission critical data, which defines who has access to specific protected files/folders and what operations) 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 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.

Category	Requirement	Thales TCT Solutions
PROTECT **Data Security (PR.DS)**	PR.DS-1: Data-at-rest is protected.	**The CipherTrust Data Security Platform** unifies data discovery, classification, data protection, and unprecedented granular access controls with centralized key management – all on a single platform. This results in fewer resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your agency. • **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 mission critical data on a per process basis. It allows administrators to alert/block suspicious activity before ransomware can take hold of your endpoints/servers. • **CipherTrust Transparent Encryption** delivers data at rest encryption, privileged user access controls and detailed data access audit logging without requiring changes to existing applications. It enables IT organizations to setup policies to prevent rogue processes and unauthorized users from encrypting your most sensitive data and prevent sensitive data exposure upon exfiltration, thereby protecting organizations from ransomware attacks. Agents protect data in files, volumes, and databases on Windows, AIX and Linux OS's across physical and virtual servers in cloud and big data environments. • **CipherTrust Application Data Protection** delivers crypto functions such as key management, signing, hashing, and encryption services through APIs, so that developers can easily secure data at the application server or big data node. • **CipherTrust Tokenization** offers both vaulted and vaultless solutions and can help reduce the cost and complexity of complying with data security mandates such as PCI DSS. • **CipherTrust Database Protection** solutions integrate data encryption for sensitive fields in databases with secure, centralized key management and without the need to alter database applications. CipherTrust Database Protection solutions support Oracle, Microsoft SQL Server, and IBM DB2 and Teradata databases. • **CipherTrust Manager is the central management point for the platform**. It enables organizations to centrally manage encryption keys, provide granular access controls, and configure security policies. It manages key lifecycle tasks including generation, rotation, destruction, import, and export; provides role-based access control to keys and policies; supports robust auditing and reporting; and offers developer-friendly REST APIs. It is available in physical and virtual form-factors that are FIPS 140-2 compliant up to level 3. **Luna Hardware Security Modules** generate, store, protect, and manage cryptographic keys used to secure sensitive data and critical applications. Luna HSMs offer the most certifications in the industry including Common Criteria, FIPS 140 Level 3, ITI and more. Have complete trust in your infrastructure, backed by a certified HSM cryptographic foundation that is internationally recognized. Thales TCT Luna HSMs provide a root of trust for existing and emerging technologies including Public Key Infrastructure (PKI), and secure store keys for code signing to maintain code integrity. Thales TCT also offers an enterprise custom-tailored code signing solution built on Luna HSMs, containers, and REST APIs, available on-premises, as a Cloud HSM service, and across hybrid environments.

Category	Requirement	Thales TCT Solutions
PROTECT Data Security (PR. DS)	PR.DS-2: Data-in-transit is protected.	**Thales High Speed Encryptors** offer the ideal certified and proven solution for data-in-motion security, including time-sensitive voice and video streams, for enterprises and government organizations: • CN series network encryptors are hardware network appliances that deliver network layer independent (Layers 2, 3 and 4) encryption for data in transit. These hardware encryptors are certified for FIPS 140-2 Level 3, Common Criteria, NATO, and are on the DoDIN APL. • CV series is a hardened virtual appliance that delivers robust encryption for data-in-motion, across high speed carrier WANs and SD-WAN links, using Network Function Virtualization (NFV).
RESPOND (RS) Mitigation (RS-MI)	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	**CipherTrust Intelligent Remediation** integrates risk-based sensitive data discovery with policy-based transparent encryption to automatically mitigate risk of data exposure. It helps organizations to visualize risks and automate remediation actions to protect against ransomware attacks. **SafeNet Trusted Access** allows organizations to respond and mitigate the risk of ransomware by providing an immediate, up to date audit trail of all access events to all systems. Extensive automated reports document all aspects of access enforcement and authentication. In addition, the service automatically streams logs to external SIEM systems.

A comprehensive set of solutions to meet NIST's Cybersecurity Framework

While Thales TCT solutions provide some of the most important capabilities in the NIST cybersecurity framework, no single company can provide a truly comprehensive set of solutions to meet the NIST requirements. That is why Thales has over 400 partners, who are among the leading technology providers in the world, to provide customers with a comprehensive set of solutions and integrations to meet NIST's Cybersecurity Framework. Please contact us to know more about how we can help you prevent not only ransomware, but destructive malware, insider threats and other Advanced Persistent Threats.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.
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