cpl.thalesgroup.com

THALES
Building a future we can all trust

Soluções da Thales para prevenir ataques ransomware

Mapeamento das soluções da Thales para a Estrutura de Cibersegurança e Guia de Prevenção de Ransomware do NIST

Os ataques ransomware são um problema há anos, mas recentemente se tornaram muito mais prejudiciais, com criminosos visando tudo, desde infraestrutura crítica até hospitais e varejistas, e exigindo dezenas de milhões de dólares como resgate. Hoje, com líderes globais discutindo esses ataques em cúpulas de alto nível, as agências governamentais estão assumindo um papel ativo em ensinar e fornecer recursos para que empresas e organizações se protejam dos ataques.

Guia de Prevenção de Ataques do NIST

O National Cybersecurity Center of Excellence (NCCoE), sob os auspícios do Nacional Institute of Standards and Technology (NIST), divulgou orientações sobre a identificação e proteção de dados contra ransomware. A Cybersecurity Special Publication (SP) 1800-25 estabelece as etapas para se ter uma estratégia abrangente para proteção de dados. Mostra também que não há bala de prata para tratar da ameaça do ransomware.

Soluções da Thales para prevenir ransomware

As soluções de segurança de dados e gerenciamento de acesso da Thales fornecem alguns dos componentes mais essenciais da estrutura de cibersegurança proposta pelo NIST para proteger empresas contra ransomware. O portfólio líder do setor da Thales oferece às empresas os seguintes recursos:

- Descoberta de dados confidenciais e classificação de acordo com o risco
- Implementação de um forte controle de identidade e gerenciamento de acesso
- Proteção e controle de dados confidenciais em repouso e em trânsito através de criptografia e tokenização
- Monitoramento da segurança dos dados para uma remediação inteligente

A seguir, um esboço de como nossas soluções mapeiam a Estrutura de Cibersegurança e o Guia de Prevenção de Ransomware do NIST:

Mapeamento das soluções da Thales para a Estrutura de Cibersegurança e Guia de Prevenção de Ransomware do NIST

Categoria	Requisito	Soluções Thales
IDENTIFICAÇÃO **Avaliação de risco**	ID.RA-1: as vulnerabilidades dos dados são identificadas e documentadas.	**O CipherTrust Data Discovery and Classification localiza dados confidenciais regulamentados, tanto estruturados como não estruturados, em nuvem, big data, e repositórios de dados tradicionais.** Um único painel de controle permite compreender os dados confidenciais e seus riscos, permitindo melhores decisões para resolver problemas de segurança, violações de conformidade e a priorizando a reparação.
PROTEÇÃO **Controle de acesso (PR.AC)**	PR.AC-1: as identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados. PR.AC-3: o acesso remoto é gerenciado. PR.AC-4: as permissões e autorizações de acesso são gerenciadas, incorporando os princípios de menor privilégio e separação de tarefas.	**O SafeNet Trusted Access fornece gerenciamento centralizado de acesso** que permite às empresas utilizar políticas consistentes de autenticação através de plataformas, automatizando e simplificando a implantação e o gerenciamento de um acervo distribuído de tokens, enquanto protege um amplo espectro de recursos, seja no local, na nuvem ou em ambiente virtual. **O SafeNet Trusted Access também fornece autenticação multifator comercial pronta para uso** com a mais ampla variedade de métodos de autenticação e fatores de forma. Isso permite que os clientes lidem com vários casos de uso, níveis de confiança e vetores de ameaças com políticas unificadas e gerenciadas centralmente - gerenciadas a partir de um back-end de autenticação oferecido na nuvem ou no local. **O CipherTrust Transparent Encryption fornece controles de acesso refinados** para dados críticos de sua empresa que definem quem tem acesso a específicos arquivos/pastas protegidos e quais operações os funcionários podem realizar. • Impeça que usuários administrativos explorem seus privilégios para obter acesso de leitura a arquivos ou bancos de dados confidenciais. • Coloque políticas rígidas de controle de acesso para arquivos de backup e criptografe os backups para evitar a exfiltração de dados. • Implemente a separação de funções de modo que os usuários do banco de dados possam ter acesso de leitura/gravação, enquanto o software de backup só tem acesso de leitura ao mesmo banco de dados.

Categoria	Requisito	Soluções Thales
PROTEÇÃO **Segurança de dados**	PR.DS-1: dados em repouso protegidos.	**A plataforma de segurança CipherTrust Data Security Platform** unifica a descoberta e classificação de dados, proteção de dados e controles de acesso granular sem precedentes com gerenciamentos de chaves centralizado, tudo em uma única plataforma. Isto resulta em menos recursos dedicados às operações de segurança de dados, controles de conformidade onipresentes e risco significativamente reduzido em todo o seu negócio. • **O CipherTrust Transparent Encryption** realiza criptografia de dados em repouso, controles de privilégio de acesso de usuário e registro de auditoria de acesso sem exigir alterações nos aplicativos existentes. Ele permite que as empresas de TI definam políticas para evitar processos invasores e usuários não autorizados de criptografar seus dados mais confidenciais e impede a exposição de dados sensíveis na exfiltração, protegendo assim as organizações de ataques ransomware. Os agentes protegem dados de arquivos, volumes e bases de dados em sistemas operacionais Windows, AIX e Linux através de servidores físicos e virtuais em ambientes de nuvem e de big data. • **O CipherTrust Application Data Protection** fornece funções criptográficas como gestão de chaves, assinatura, hashing e serviços de criptografia através de APIs, para que os desenvolvedores possam facilmente proteger dados no servidor do aplicativo ou em nodes de big data. • **O CipherTrust Tokenization** é oferecido tanto com e sem vault e pode ajudar a reduzir o custo e a complexidade do cumprimento de mandatos de segurança de dados como o PCI-DSS. • **As soluções CipherTrust Database Protection** integram a criptografia de dados para campos especiais de bases de dados com gestão de chaves segura e centralizada e sem necessidade de alterar aplicações de bases de dados. As soluções CipherTrust Database Protection suportam bancos de dados Oracle, Microsoft SQL Server, IBM DB2 and Teradata. • **O CipherTrust Manager é o ponto de gerenciamento central da plataforma**. Trata-se de uma solução de gerenciamento de chaves empresariais líder da indústria para gerenciar de maneira centralizada chaves de criptografia e configurar políticas de segurança. Ele gerencia tarefas do ciclo de vida de chaves, incluindo geração, rotação, destruição, importação e exportação, fornece controle de acesso baseado em funções a chaves e políticas, suporta auditorias e relatórios robustos, e oferece APIs REST amigáveis ao desenvolvedor. Ele está disponível em formato físico e virtual que estão em conformidade com o FIPS 140-2 até o nível 3. Os **Módulos de Segurança de Hardware Luna** geram, armazenam, protegem e gerenciam chaves criptográficas usadas para proteger dados confidenciais e aplicativos críticos. Os HSMs Luna oferecem a maioria das certificações do setor, incluindo Common Criteria, FIPS 140-2 de nível 3, ITI e outras. Tenha total confiança em sua infraestrutura com o suporte de uma base criptográfica de HSMs certificados que é reconhecida internacionalmente. Os HSMs Luna da Thales fornecem uma base de confiança para tecnologias existentes e emergentes, incluindo Infraestrutura de Chaves Públicas (PKI) e armazenamento seguro de chaves para assinatura de código a fim de manter a integridade do código. A Thales também oferece uma solução de assinatura de código personalizada para empresas que é integrada em HSMs Luna, containers e APIs REST e está disponível no local, como um serviço de HSM para nuvem, e em ambientes híbridos. **A Thales Data Protection on Demand** é uma plataforma em nuvem que oferece uma ampla gama de serviços de segurança de hardware e gerenciamento de chaves em nuvem através de um simples mercado online.

Categoria	Requisito	Soluções Thales
PROTEÇÃO **Segurança de dados**	PR.DS-2: os dados em trânsito são protegidos.	Os **Thales High Speed Encryptors** oferecem a solução ideal certificada e comprovada para a segurança de dados em movimento, incluindo transmissão de voz e vídeo sensíveis em tempo real para empresas e organizações governamentais: • Os encriptadores de rede da série CN são dispositivos de hardware de rede que fornecem criptografia independente para camadas de rede (camadas 2, 3 e 4) de dados em trânsito. Estes encriptadores de hardware possuem certificação FIPS 140-2 de nível 3, Common Criteria, NATO, e estão no DoDIN APL. • A série CV é um dispositivo virtual reforçado que fornece criptografia robusta para dados em movimento através de WANs de alta velocidade e links SD-WAN utilizando a Network Function Virtualization (NFV).
RESPOSTA (RS) **Mitigação (RS-MI)**	RS.MI-3: as vulnerabilidades recentemente identificadas são mitigadas ou documentadas como riscos aceitos.	○ **CipherTrust Intelligent Remediation** integra a descoberta de dados confidencias baseados em risco com criptografia transparente baseada em políticas para mitigar automaticamente o risco de exposição de dados. Isso ajuda as empresas a visualizar os riscos comerciais e automatizar as ações de remediação para proteção contra ataques ransomware. ○ **SafeNet Trusted Access** permite que as empresas respondam e mitiguem o risco de ransomware, fornecendo um registro de auditoria imediato e atualizado de todos os eventos de acesso a todos os sistemas. Relatórios automáticos abrangentes documentam todos os aspectos da imposição e autenticação de acesso. Além disso, o serviço transmite automaticamente os registros para sistemas SIEM externos.

Um conjunto abrangente de soluções para estar em conformidade com a Estrutura de Cibersegurança do NIST

As soluções Thales fornecem algumas das capacidades mais importantes da estrutura de cibersegurança do NIST, mas nenhuma empresa sozinha pode fornecer um conjunto verdadeiramente abrangente de soluções para atender aos requisitos do NIST. É por isso que a Thales tem mais de 400 parceiros, que estão entre os principais fornecedores de tecnologia do mundo, para fornecer aos clientes um conjunto abrangente de soluções e integrações para estar em conformidade com a Estrutura de Cibersegurança do NIST. Entre em contato conosco para saber mais sobre como podemos ajudar a evitar não apenas ataques ransomware, mas também malwares destrutivos, ameaças internas e outras Ameaças Persistentes Avançadas.

Sobre a Thales

A Thales é líder mundial em segurança de dados e tem a confiança dos governos e das empresas mais reconhecidas em todo o mundo para ajudar a proteger seus dados mais confidenciais. As pessoas em quem você confia para proteger sua privacidade confiam na Thales para proteger seus dados. Em termos de segurança de dados, as organizações enfrentam cada vez mais momentos decisivos. Seja na criação de uma estratégia de criptografia, migração para a nuvem ou cumprimento de normas de conformidade, você pode confiar na Thales para proteger sua transformação digital.