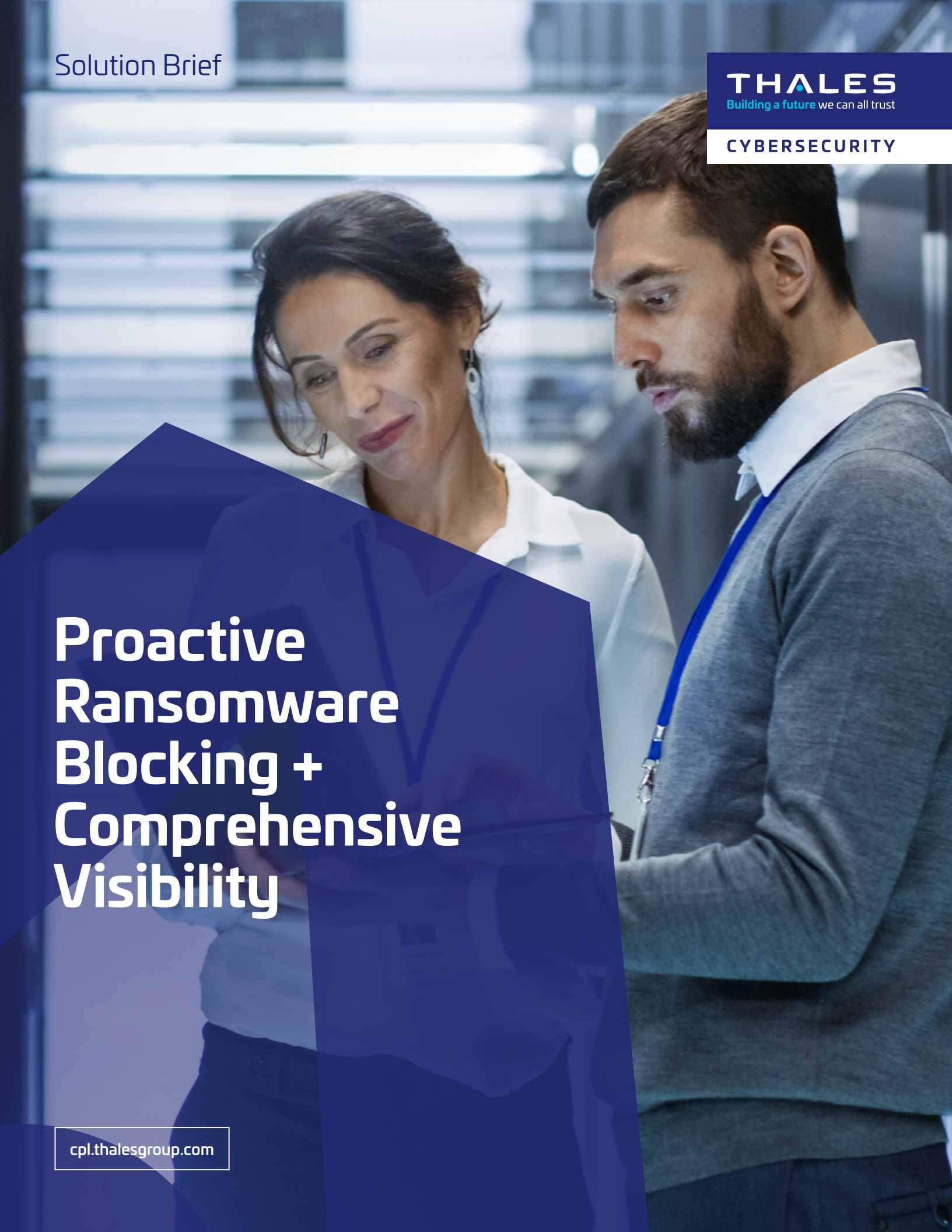
Solution Brief

THALES
Building a future we can all trust

CYBERSECURITY



Proactive Ransomware Blocking + Comprehensive Visibility

cpl.thalesgroup.com

THALES
Building a future we can all trust

CYBERSECURITY

Advanced Ransomware Defense

CipherTrust Ransomware Protection + Data Security Fabric

Ransomware attacks surged 49% in the first half of 2025, with average costs now exceeding $5.13 million. Modern ransomware groups have shifted to sophisticated data exfiltration strategies—90% of attacks now involve data theft, up from just 10% in 2019. Traditional security tools either protect data without detecting ransomware activity or monitor misuse only after files are encrypted. Organizations need a solution that stops malicious encryption attempts before they succeed while providing comprehensive monitoring for regulatory compliance.

CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) and Data Security Fabric (DSF) create a powerful defense by combining active attack prevention with real-time observability and threat detection across your data infrastructure - addressing critical regulatory requirements while stopping ransomware before it can take hold.

Challenge: Ransomware Blocks Access to Business-Critical Data

Modern Ransomware: A Multi-Faceted Threat

Organizations face average downtimes of 24 days, with 60% experiencing revenue loss and 53% suffering brand damage following attacks. The threat landscape has evolved beyond simple file encryption to sophisticated multi-extortion strategies that target both operational continuity and data confidentiality.

The Compliance Challenge

Enterprises manage data across hybrid, multi-cloud, and legacy systems while facing mounting regulatory requirements. Organizations cannot afford siloed tools when threats can emerge anywhere across their data estate, and compliance frameworks increasingly require both data protection and comprehensive monitoring capabilities.

Traditional Defenses Fall Short

Most security tools either protect data without detecting ransomware activity or detect misuse only after damage is done. Ransomware can encrypt critical files in seconds, while insider threats and misconfigurations often bypass traditional defenses. Organizations need a solution that can stop malicious encryption attempts before they succeed, while also providing the visibility, detection, and audit evidence required to protect sensitive data and meet regulatory requirements.

Solution: Ransomware Defense

CTE-RWP detects and blocks unauthorized processes attempting to encrypt data, stopping ransomware before it takes hold through behavioral analysis and machine learning. DSF adds real-time monitoring, anomaly detection, and audit-ready visibility across data sources, delivering an integrated defense that combines active prevention with comprehensive data security monitoring. application-to-data security coverage. Existing native database encryption can be enhanced by adding CipherTrust Cloud Key Management for robust, centralized, and automated key lifecycle management.

+

CipherTrust Ransomware Protection

Data Security Fabric

CipherTrust Ransomware Protection	Data Security Fabric
• **Behavioral Detection & Blocking** • Process-based machine learning models • Dynamic detection of suspicious file I/O activity • Proactive blocking before encryption occurs • Minimal configuration required	• **Comprehensive Data Monitoring** • Real-time analytics across sensitive data • Automated data classification and discovery • Enterprise-scale risk prioritization • AI/ML-behavioral anomaly and threat detection

Key Advantages

Transparent Data Protection

CTE-RWP continuously enforces ransomware protection per volume with minimal configuration and no modification to applications. It monitors abnormal file activity caused by ransomware-infected processes and alerts/blocks when detected.

Broadest Coverage

DSF provides comprehensive coverage across multi-cloud, hybrid, and on-premises environments, protecting over 500,000 business critical databases. The platform monitors 1,500 file formats, data types, and cloud assets with 300 data repositories achieving 100% coverage.

Easy to Deploy

Start with ransomware protection alone without setting up restrictive access control policies. CTE-RWP enables immediate protection while DSF delivers comprehensive monitoring without requiring extensive configuration.

Robust Detection Capabilities

Combined solution uses process-based machine learning models and behavioral analytics to dynamically detect suspicious activity across both structured and unstructured data sources.

Business Impact

Extensive Ransomware Defense

- **Prevention:** Behavioral detection blocks unauthorized encryption before damage occurs
- **Detection:** Real-time monitoring identifies evolving threats and anomalous activity
- **Compliance:** Automated audit trails satisfy regulatory requirements across multiple frameworks

Operational Benefits

- Reduced vendor sprawl through integrated approach
- Simplified management with complementary platforms
- Faster compliance reporting - tasks reduced from days to minutes

Compliance & Regulatory Benefits

Multi-Framework Coverage

Support key HIPAA, PCI DSS, SOX, GDPR, NIS2, and DORA requirements with integrated ransomware protection and data monitoring that strengthens your compliance posture.

Automated Compliance Reporting

DSF streamlines data-related compliance processes, reducing manual labor and providing easy access through interactive tools. Tasks that formerly required days can be executed in minutes, significantly reducing compliance overhead costs.

Audit-Ready Evidence

Combined solution provides comprehensive audit trails and compliance reports that satisfy requirements for data protection monitoring across multiple regulatory frameworks.

Deployment Scenarios

For those organizations currently deploying DSF or legacy database activity monitoring tools, extend monitoring capabilities with CTE-RWP to add ransomware prevention as a natural complement to existing data visibility and compliance monitoring. CTE-RWP is a huge step in managing your risks of a ransomware attack.

For those organizations currently using CTE-RWP, strengthen ransomware protection by pairing prevention with comprehensive data monitoring, enabling audit trails and compliance reporting alongside threat blocking.

For those organizations who are just getting started, implementing data protection and monitoring from a single vendor unifies prevention and detection– can reduce recovery costs, accelerate compliance readiness, and minimize operational disruption. The best defense against ransomware is multiffaceted. Adding CipherTrust Transparent Encryption (CTE) provides additional benefits to guard against ransomware including access policies to reduce risk factors caused by potential attacks.

By combining CTE-RWP's behavioral ransomware protection with DSF's comprehensive data monitoring, organizations gain complementary capabilities that strengthen their overall data security posture. With extensive integrations spanning enterprise databases, cloud platforms, and security infrastructure, organizations can deploy consistent protection and monitoring policies across their entire data landscape.

Advanced capabilities including process-level ransomware blocking, automated compliance reporting, and behavioral analytics provide the intelligent threat response needed for modern data security challenges. Backed by Thales' proven cryptographic expertise and data security leadership, this combined solution delivers a strategic foundation for comprehensive data security posture management with enterprise-grade operational simplicity.

Get Started Today

Contact your Thales representative today to discover how CTE-RWP and DSF work together to stop ransomware attacks before they succeed while delivering comprehensive data monitoring and automated compliance reporting across your enterprise.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us