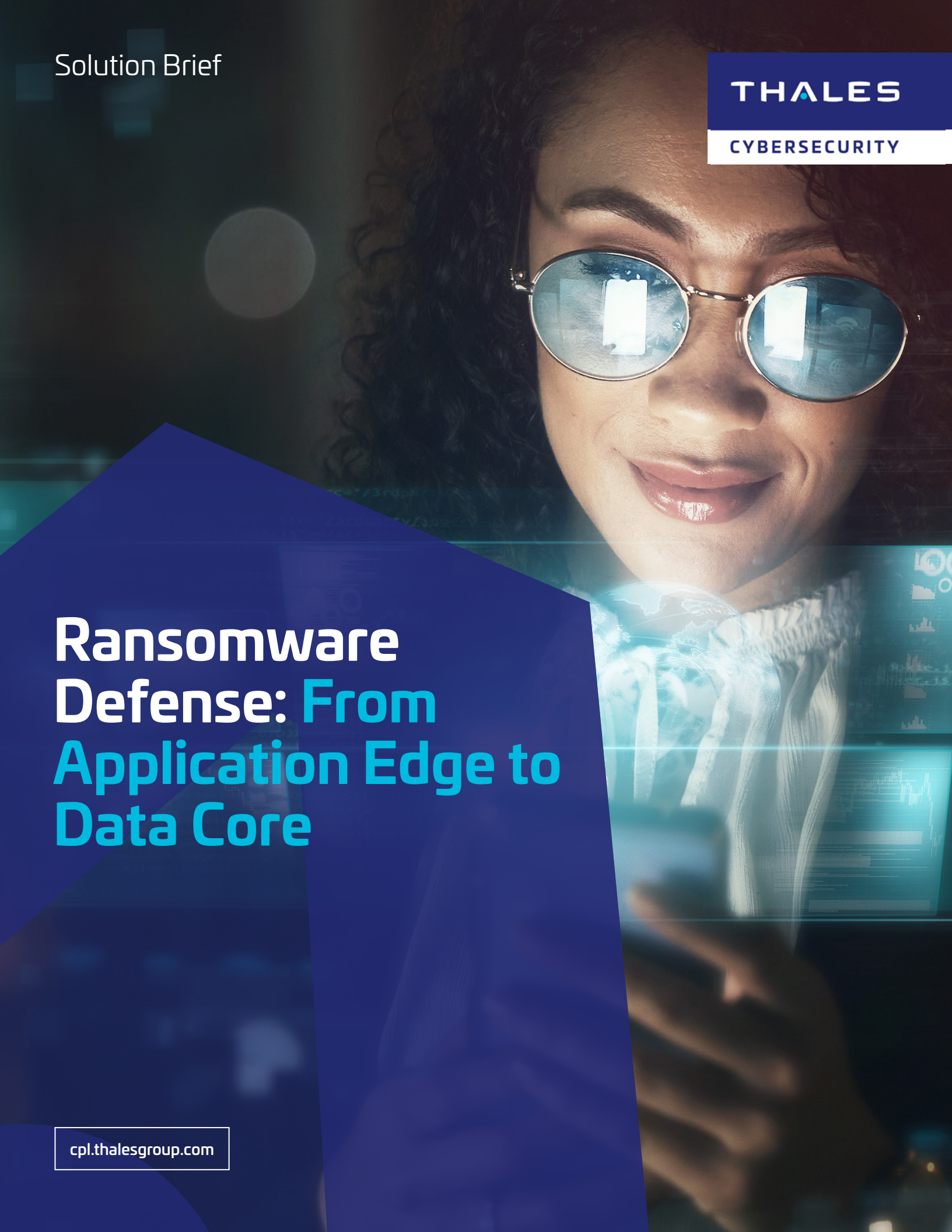
Solution Brief

THALES
CYBERSECURITY



Ransomware Defense: From Application Edge to Data Core

cpl.thalesgroup.com

THALES
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.

Beyond data layer protection, Imperva API Security and Advanced Bot Protection (ABP) extend the combined CTE-RWP and DSF solution to the application edge, sealing common ransomware entry points at web and API tiers. They prevent bot driven reconnaissance attacks, credential abuse, and API exploitation before attackers can reach databases and file shares protected by CipherTrust and monitored by Data Security Fabric

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.

Application-Edge Sealing

Imperva API Security and Advanced Bot Protection close web/API entry points that ransomware groups exploit for initial access, credential abuse, and command-and-control, extending CTE-RWP/DSF protection from data core to perimeter.

Zero-Config Bot & API Defense

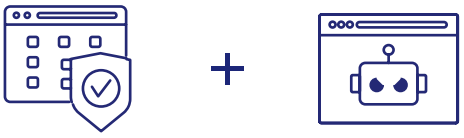
Automatically discovers shadow APIs and detects human-like automation with minimal setup, blocking sophisticated threats that bypass traditional WAF/DDoS while preserving legitimate traffic.

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.



API Security + **Advanced Bot Protection**

API Security	Advanced Bot Protection
• Discovers and classifies managed and shadow APIs • Enforces strong authentication and governance • Uses behavioral analytics to block anomalous API calls linked to ransomware command-and-control, lateral movement, or data staging	• Detects and stops human-like bots driving credential stuffing, scanning, and exploit attempts • Blocks malicious automation before it can gain initial access or spread ransomware • Protects against web scraping, account takeover, scalping, transaction fraud, gift card fraud, denial of service, competitive data mining, unauthorized vulnerability scans, spam, click fraud, and web and mobile API abuse • Integrates with API Security to provide comprehensive protection of your most critical APIs • Human expertise with a dedicated bot-focused analyst team

Robust Detection Capabilities

The combined solution uses process-based machine learning models and behavioral analytics to dynamically detect suspicious activity across both structured and unstructured data sources. Correlates application-edge bot/API events with DSF monitoring and CTE-RWP blocks for unified visibility, faster investigations, and comprehensive audit trails across the full attack chain.

Business Impact

Extensive Ransomware Defense

- Prevention: Behavioral detection blocks unauthorized encryption before damage occurs, while API Security and ABP prevent initial access, command-and-control, and automated delivery of ransomware payloads over web and API channels.
- Detection: Real-time monitoring identifies evolving threats and anomalous activity across databases and file repositories, augmented by application-edge detection of suspicious API and bot activity that often signals early-stage ransomware operations
- Compliance: Automated audit trails and unified observability from application to data help satisfy regulatory requirements for controlling access, data movement, and high-risk automation across multiple frameworks

Operational Benefits

- Reduced vendor sprawl
- 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

The solutions provide comprehensive audit trails and compliance reports that satisfy requirements for data protection monitoring across multiple regulatory frameworks.

Deployment Scenarios

Core Ransomware Defense (CTE-RWP + DSF)

Deploy CipherTrust Ransomware Protection for behavioral file encryption blocking paired with Data Security Fabric for real-time monitoring and compliance across databases and files. Ideal for organizations prioritizing data-layer protection with immediate ransomware prevention and audit-ready visibility.

For those organizations who have or are currently replying DSF, 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.

Layered Data Security: Flexible Protection from Edge to Core

Extend the core stack with Imperva API Security to govern shadow APIs and block command-and-control/lateral movement, plus Advanced Bot Protection to stop human-like automation, credential stuffing, and initial access attempts at the application edge. Delivers end-to-end coverage from perimeter bots to data core, unifying threat blocking, detection, and compliance in one ecosystem

For organizations just getting started, implementing CTE-RWP, DSF, API Security, and Advanced Bot Protection from a single vendor unifies prevention and detection from perimeter to data core—reducing recovery costs, accelerating compliance readiness, and minimizing disruption. The best defense against ransomware is multifaceted, with CTE adding access policies to further reduce attack risks.

By combining CTE-RWP's behavioral ransomware blocking, DSF's comprehensive data monitoring, API Security's shadow API governance, and ABP's human-like bot mitigation, organizations gain complementary capabilities across their entire data landscape—from enterprise databases and cloud platforms to web/API entry points.

Advanced capabilities like process-level blocking, automated compliance reporting, behavioral analytics, and edge-layer threat sealing deliver intelligent response for modern challenges. Backed by Thales' cryptographic expertise, this solution provides a strategic foundation for data security posture management with enterprise-grade simplicity.

- If you already use CTE-RWP, adding DSF improves visibility, compliance reporting, and threat detection—no need to change your applications.
- Using Imperva API Security or ABP at the edge? Pairing them with CTE-RWP adds strong data-layer protection against ransomware and automated attacks on file systems and servers.
- Even just combining two components (like CTE-RWP + DSF) gives noticeable benefits.
- The complete solution extends protection from web and API entry points to critical data, without requiring an "all or nothing" approach.

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.