WHITE PAPER

Mitigating the Impact of Ransomware Attacks With Entrust

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

Overview

The Ever-Growing Threat of Ransomware

The threat of ransomware attacks has grown steadily over the last several years. Industry research indicates that organizations across all sectors now face ransomware as a persistent and accelerating risk. Attacks are becoming more frequent, more targeted, and more damaging, with cloud adoption and distributed IT environments introducing new attack surfaces. AI is also lowering the barrier to entry for ransomware attacks while automating key stages of the attack lifecycle, from initial access to data exfiltration.

The financial impact of ransomware continues to rise sharply. Beyond ransom payments themselves, organizations must absorb the cost of operational downtime, incident response services, regulatory penalties, and long-term reputational damage. As attackers increasingly combine data encryption with data exfiltration, ransomware has evolved from a purely operational threat into a major business and compliance risk.

This white paper examines the multifaceted challenges posed by modern ransomware and explains how Entrust can mitigate the impact of both data encryption and data exfiltration attacks through advanced data resilience, integrity controls, and self-healing capabilities.

The Multifaceted Threat of Ransomware

Loss of Data and Data Access

The most familiar consequence of a ransomware attack is the loss of access to mission critical data. By encrypting data stores, attackers can bring entire applications, systems, and business services to a halt. Even when organizations choose to pay a ransom, full data recovery is rarely guaranteed, and prolonged downtime can result in significant financial loss.

When Ransomware Goes Undetected

Modern ransomware variants are increasingly adept at evading traditional detection mechanisms. These threats may remain dormant inside an environment, spreading laterally and infecting backups before triggering encryption. Some variants deliberately target backup systems, reducing the effectiveness of conventional recovery strategies and increasing pressure on victims to pay.

Double Extortion and Data Exfiltration

In double extortion attacks, ransomware operators exfiltrate sensitive data prior to encryption and threaten public disclosure if payment is not made. This approach increases leverage over victims and introduces regulatory, legal, and reputational consequences even if systems are restored. As a result, protecting data confidentiality has become as critical as maintaining data availability.

A Thriving Ransomware Ecosystem

The rise of ransomware-as-a-service (RaaS), combined with improved phishing techniques and automation powered by AI, has lowered the barrier to entry for cybercriminals. Organized ransomware groups now operate with professionalized tools, established supply chains, and deep knowledge of enterprise infrastructure, reinforcing the reality that ransomware is no longer a matter of "if," but "when."

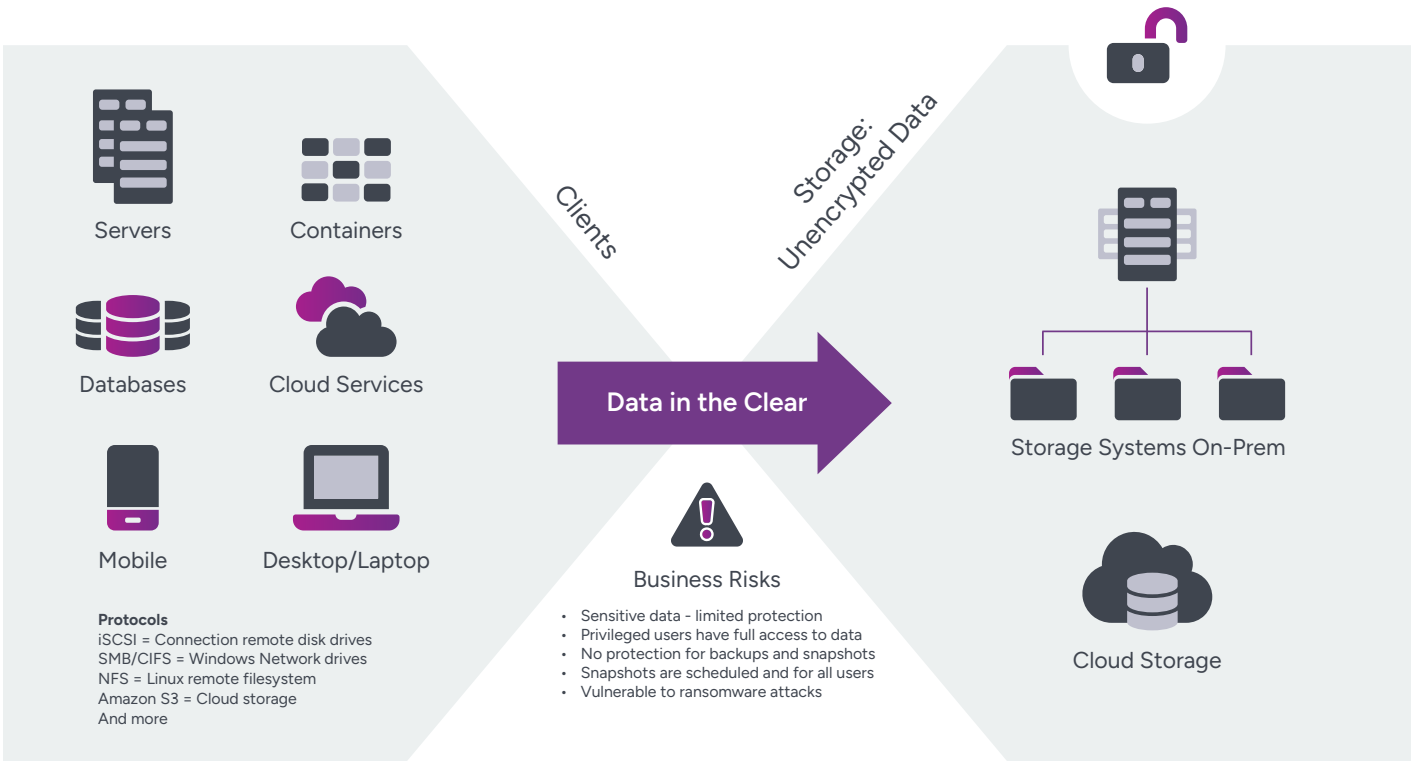

Figure 1: Illustration highlighting how client data being routed to backup is exposed in the clear

Mitigating Ransomware Attacks With Entrust File Encryption

The Entrust File Encryption solution is designed to reduce the operational, financial, and security impact of ransomware attacks by ensuring data resilience, integrity, and confidentiality across on-premises, cloud, and hybrid environments.

Robust Data Resilience to Maintain Access During an Attack

Entrust delivers high availability and data integrity controls that help organizations maintain access to critical data even during an active ransomware incident. Each Entrust deployment operates as a virtual cluster that can be deployed on premises, in public cloud environments, or across hybrid and multi-cloud architectures.

Multiple virtual clusters can be configured for failover, providing resilience across geographically distributed environments and minimizing single points of failure.

Automatic Data Migration to Prevent Repeated Attacks

Entrust supports automated data migration to alternate storage locations when integrity thresholds are breached. If a defined number of data integrity checks fail within a specified time window, data can be automatically migrated from a primary storage tier to a secondary, secure location. This process occurs transparently in the background, without downtime, enabling rapid containment and continued operations.

Automatic Self-Healing to Reconstruct Compromised Data

When data is altered, encrypted, or deleted as a result of ransomware or other malicious activity, Entrust's File Encryption self-healing capabilities automatically reconstruct affected data using trusted fragments stored across multiple locations. This process is transparent to applications and users, allowing organizations to maintain business continuity while remediation activities are underway.

Immutable Storage Interfaces and Point-in-Time Rollback

Credential abuse is a common entry point for ransomware attacks. Entrust mitigates this risk through immutable storage interfaces and object-locking capabilities that prevent unauthorized modification of protected data.

In the event of a credential-based attack, organizations can roll data back to a known good point in time prior to the incident, significantly reducing reliance on time-consuming, last-resort backup recovery processes.

Automated Alerts for Early Detection

When a storage location fails a data integrity health check, the Entrust platform automatically generates alerts for security operations teams. These alerts act as early warning signals, enabling faster detection, investigation, and response and reducing the likelihood that ransomware activity will go unnoticed.

Protection Against Data Exfiltration

Entrust File Encryption mitigates double extortion ransomware by rendering data unintelligible to unauthorized parties. Even if attackers gain direct access to underlying storage systems, exfiltrated data cannot be reconstructed or exploited without proper authorization. This ensures that sensitive information remains protected from disclosure, sale, or extortion.

Advanced file-level protection safeguards data privacy regardless of where data is stored, helping organizations meet regulatory and compliance requirements while reducing exposure during an attack.

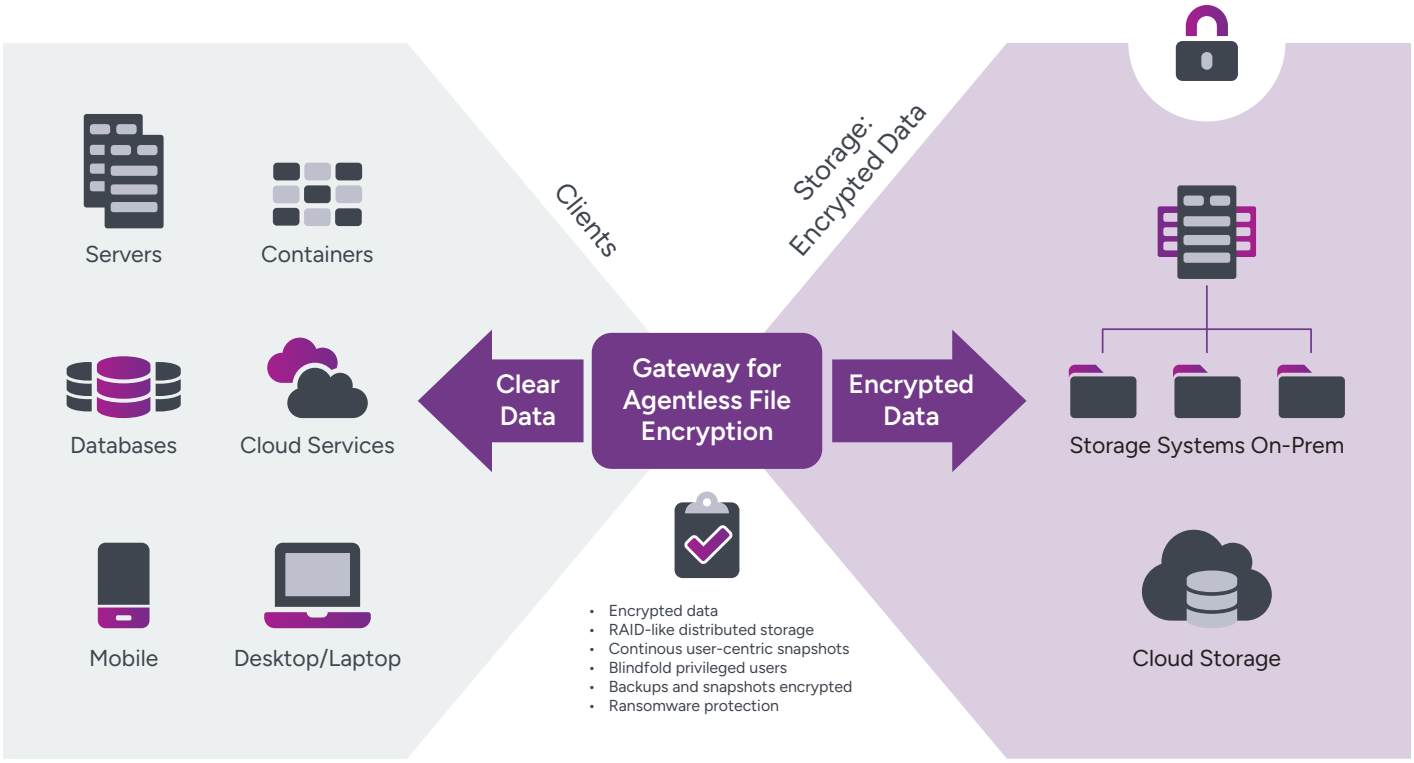

Figure 2: Illustration of file-level encryption applied by gateway

Unified, Multi-Protocol Platform Across Multiple Clouds

The Entrust solution provides agentless integration and centralized management without requiring changes to application behavior or data flows. It is infrastructure and vendor-agnostic, operating transparently alongside existing services.

Support for S3 compatible APIs, SMB/NFS, and iSCSI interfaces enables seamless migration with minimal configuration changes. As a result, Entrust's File Encryption solution minimizes operational overhead for development and IT teams while delivering continuous, zero-downtime data protection.

Conclusion

As ransomware attacks continue to increase in scale, frequency, and sophistication, organizations must adopt proactive strategies to protect data availability, integrity, and confidentiality.

The Entrust platform mitigates the impact of ransomware through robust data resilience, automatic self-healing, immutable storage controls, real-time security alerts, and protection against data exfiltration. Together, these capabilities help organizations reduce downtime, limit financial losses, and protect their reputation in the face of modern ransomware threats.

To learn more about Entrust File Level Encryption, visit: **www.entrust.com/products/cryptographic-security-platform/agentless-file-encryption**.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit **entrust.com.**

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION