riverbed

SOLUTION BRIEF

Unlocking Performance Without Undermining Security

Accelerating Encrypted Traffic with Riverbed Keystone Server

The Value: Why Decrypting for Optimization Matters

Encryption protects data—but obscures performance opportunities. Applications from analytics to cloud workloads now depend on rapid, reliable data flow. Slow movement creates system bottlenecks, drives up infrastructure costs and limits scalability.

When TLS-encrypted traffic can be decrypted and optimized in a controlled way, organizations gain measurable benefits:

- Faster performance for SaaS and cloud applications
- Improved end-user experience and productivity
- Reduced WAN utilization and cost
- Better ROI from existing network infrastructure

The value is significant—but only if decryption is done in a way that security teams trust. This is not a radical idea. Enterprises already decrypt TLS traffic every day to:

- Inspect traffic with firewalls
- Enforce policy with secure web gateways
- Distribute traffic with load balancers

Keystone: Purpose-Built to Decrypt TLS Traffic for Optimization

With Keystone server, Riverbed becomes an integral part of your security infrastructure, with specific controls for security personnel. Using the same accepted security methods as firewalls and load balancers, this enables you to accelerate practically all encrypted traffic, which could substantially increase your acceleration footprint.

Business Challenge

Today, the vast majority of enterprise application traffic is encrypted with TLS. SaaS platforms, cloud services, collaboration tools and web applications all rely on encryption by default. This is essential for security—but it has a direct impact on network performance.

When traffic is encrypted:

- Network optimization and acceleration techniques cannot be applied
- WAN bandwidth consumption increases
- Application response times degrade
- User experience and productivity suffer

In many environments, encrypted traffic is simply bypassed by optimization systems—not because it lacks value, but because it cannot be accessed safely.

Optimization fundamentally requires visibility into application data. To accelerate TLS-encrypted traffic, the infrastructure must decrypt the traffic, apply optimization and then re-encrypt it.

The organizational challenge is the team responsible for making the network “fast” is usually different than the team responsible for making the network “safe.”

The opportunity is a solution both teams are comfortable. This is Riverbed Keystone sever.

Keystone is a centralized TLS decryption and signing service. Trust, certificate authorities and cryptographic operations are consolidated in one place and governed by security policy. This mirrors how TLS inspection is handled today in security infrastructure.

Keystone exists for one primary reason: to decrypt TLS traffic so that optimization can be applied safely and at scale. What makes Keystone different is not what it does—decrypting TLS traffic—but how it does it.

Keystone decrypts encrypted traffic using the same security models and operational patterns that enterprises already rely on. From a security standpoint, Keystone behaves like infrastructure teams already manage and approve.

Private Keys Are Never Distributed

A key expectation of security teams is that private keys must be tightly controlled.

With Keystone

- TLS private keys are generated, stored and used centrally
- Private keys never leave the Keystone service
- Network devices request cryptographic operations but never handle long-lived key material

This ensures TLS decryption for optimization does not introduce key sprawl or unmanaged risk.

Explicit, Policy-Based Decryption

Keystone does not decrypt traffic indiscriminately. Security teams define policies that determine:

- Which traffic may be decrypted
- Which applications or destinations are eligible for optimization
- Which traffic must remain encrypted end-to-end

If traffic is not explicitly approved, it is not decrypted—and therefore not optimized.

Ephemeral Certificates, Not Static Proxies Explicit, Policy-Based Decryption

Instead of static, manually managed proxy certificates, Keystone uses short-lived, on-demand TLS proxy certificates.

This approach:

- Reduces cryptographic exposure
- Simplifies certificate lifecycle management
- Allows rapid response to policy or trust changes

This aligns with modern security expectations.

Designed for Cross-Team Collaboration

Keystone removes a long-standing friction point between teams:

- Networking teams gain the ability to optimize encrypted traffic
- IT teams see better application performance and user experience
- Security teams retain full control over decryption, trust and policy

Decryption for optimization is no longer an ad-hoc exception—it is a governed, auditable security service.

Further, using Keystone with Riverbed SteelHead Acceleration supports many advanced features that security teams will appreciate, including post-quantum cryptography to protect data transfers against future quantum-enabled threats.

Keystone does not weaken encryption—it enables organizations to use decryption responsibly to recover performance and value that would otherwise be lost.

The Right Conversation to Start Now

Encrypted traffic continues to grow and performance expectations continue to rise. Ignoring encrypted traffic is no longer sustainable, but neither is bypassing security controls. Contact us to schedule a detailed SecOps-focused walkthrough, where security teams can examine TLS trust and decryption flows, key protection and lifecycle controls, and policy enforcement and auditability.

Learn more about Riverbed Acceleration at riverbed.com.