OBJECT FIRST

White Paper

Achieving Ransomware Resilience in SLED Environments

Your blueprint for cyber resilience

State, Local, and Education (SLED) IT environments face a unique convergence of challenges: safeguarding sensitive data, maintaining compliance, delivering equitable digital services, and operating within tight budgetary constraints.

The paper explores four pressing issues impacting SLED agencies today:

1. **Fragmented Infrastructure:** SLED environments often rely on a mix of legacy and modern systems that don't integrate well, complicating security and recovery.
2. **Service Accessibility Risks:** Public-facing digital services depend on resilient infrastructure and clear documentation to remain inclusive, reliable, and audit-ready.
3. **Procurement and Budget Constraints:** Complex purchasing rules and limited budgets require flexible, cost-effective solutions that align with funding cycles and compliance needs.
4. **Ransomware Vulnerability:** Legacy backup systems lack immutability and architectural separation, making them easy targets for modern ransomware attacks.

This paper presents a technical framework for addressing these demands through the Object First appliance, a ransomware-proof backup data appliance engineered specifically for Veeam, to ensure security, reduce the risk of disruption, and enable growth for businesses and people.

Interoperability and legacy integration: bridging the old and the new

SLED agencies manage a patchwork of systems, some decades old, others cloud-native. Payroll might run on a mainframe, permitting on a SaaS platform, and GIS on a custom-built tool. These systems often don't communicate, creating silos that slow down operations and increase risk.

The Integration Challenge

Replacing legacy systems is expensive and politically difficult. Many are tied to long-term contracts or compliance requirements. As a result, IT teams must integrate rather than replace them. This means building bridges between incompatible systems using middleware, service buses, and custom APIs.

Integration must be built on consistency. If systems don't share authentication, logging, or backup protocols, they become harder to secure and recover. Backup tools must be flexible enough to support this diversity without introducing complexity.

Legacy backup systems are crumbling

Many SLED organizations still rely on outdated tape systems or fragmented cloud appliances. Tapes are slow and fragile, while cloud backups introduce complexity, egress fees, and compliance challenges. Restore times are often unpredictable, and testing is frequently skipped due to staffing constraints, leaving organizations exposed when recovery matters most.

Above: An image of Spectra Logic's LTO-8 tape and tape drive, courtesy of TechTarget.

Where the Object First appliance fits in

The Object First appliance simplifies backup storage across heterogeneous environments. Its plug-and-play architecture works seamlessly with Veeam, which supports a wide range of legacy and modern systems. It takes less than 15 minutes to configure, requires zero security expertise to manage, and does not require additional setup or namespace adjustment at the Veeam layer when scaled.

There's no need to manage cloud buckets or write custom scripts. This makes it easier for SLED IT teams to protect diverse infrastructure without adding operational burden. In environments where integration is a necessity, not a choice, the Object First appliance provides a consistent, secure foundation for backup and recovery.

Accessibility and citizen/student services: infrastructure that supports equity

Public-facing digital services are now core to government and education. Citizens expect to apply for permits, pay bills, and access records online. Students rely on remote learning platforms, grade portals, and digital resources. These services must be reliable, inclusive, and available around the clock.

Designing for Everyone

Accessibility should be grounded in both compliance and equity in equal measures. ADA standards require screen reader support, keyboard navigation, and clear visual design. But accessibility also requires optimizing low-bandwidth environments, supporting mobile devices, and ensuring uptime during peak usage.

In rural or underserved areas, infrastructure limitations can make digital access difficult. IT teams must design systems that perform well even under constrained conditions. That includes resilient infrastructure and clear operational documentation that enables fast recovery and consistent service delivery. In SLED IT environments, continuity depends as much on shared knowledge as on hardware. When systems fail or audits begin, the absence of clear documentation can delay recovery and expose compliance gaps.

The infrastructure behind the interface

Front-end accessibility depends on back-end reliability. If a system goes down or a backup fails, services become inaccessible. This affects critical access to education, public safety, and civic engagement.

An example of this occurred in Australia in 2020. The country's MyGov portal crashed during a surge in demand caused by the COVID-19 pandemic, leaving thousands unable to access critical services like welfare and healthcare. Although the front-end interface was functional, the back-end infrastructure failed to handle the traffic, lacking scalability and redundancy. This outage disrupted public access to essential resources, especially for vulnerable populations, and highlighted how digital accessibility is meaningless without reliable infrastructure behind it.

Effective documentation plays a key role in maintaining uptime. Runbooks for restores, patching, and user provisioning; network diagrams that clarify dependencies and failover paths; and policy repositories that outline access controls and security protocols all help ensure that services remain available and recoverable. These resources must be centralized and version controlled. Fragmented or outdated documentation increases risk and slows response times.

Training is of equal importance. Tabletop exercises validate response plans, cross-training ensures redundancy in critical roles, and user education reduces preventable security incidents. Together, documentation and training support audit readiness and operational resilience, ensuring that accessibility isn't compromised when systems are under pressure.

Object First Mini: purpose-built backup for SLED edge environments

Government and education agencies increasingly rely on digital services to support civic engagement, remote learning, and public access. But not every environment has the infrastructure to support traditional rack-mounted backup systems. Branch offices, remote campuses, and legacy facilities often face space, cooling, and power constraints that make deployment challenging.

The Object First Mini is designed to meet these conditions head-on. Since it fits on shelves, in closets, or under desks, it's ideal for space-conscious environments. With a compact desktop form factor and low acoustic profile, it brings secure, immutable backups to locations that lack dedicated server infrastructure without compromising performance or manageability.

For information on storage options and compatibility, please refer to our datasheet.

Budget management and procurement: navigating constraints with strategy

SLED IT teams operate under tight financial constraints. Budgets are often flat or shrinking, while demands for digital services, cybersecurity, and compliance continue to grow. Procurement is governed by complex rules, and purchases must align with grant cycles, cooperative contracts, and legislative funding windows.

The Procurement Landscape

Traditional competitive bidding processes can take months. Cooperative purchasing agreements like NASPO ValuePoint and OMNIA Partners offer a faster path, allowing agencies to buy from pre-approved vendors. But even then, purchases must be justified with clear ROI and compliance alignment.

IT teams must conduct Total Cost of Ownership (TCO) analyses, explore open-source alternatives, and prioritize predictable OPEX models over large CAPEX investments. Appliances that introduce hidden costs like cloud egress fees or complex licensing are often rejected.

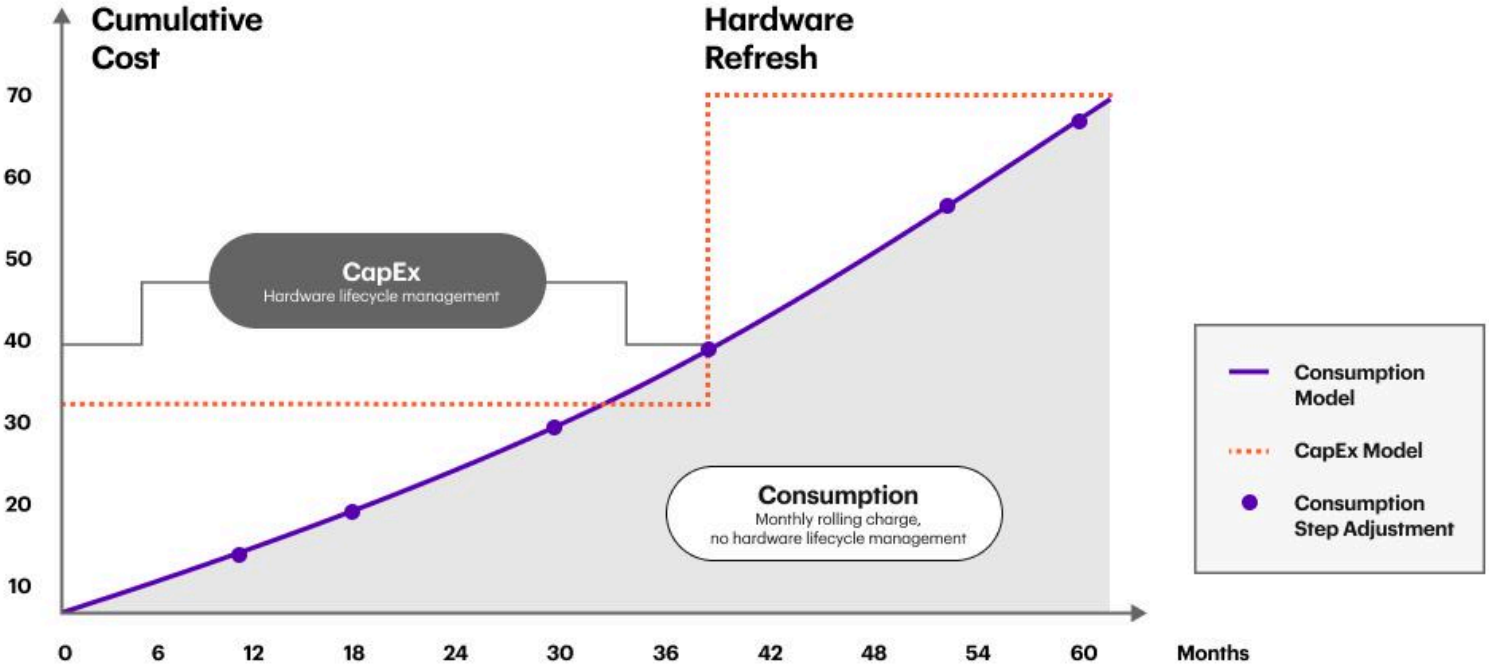
Object First value proposition: consumption model tailored for SLED

For agencies with predictable infrastructure needs and long-term planning, Object First's CapEx model offers full ownership and control through a one-time investment in backup storage hardware.

However, many SLED environments operate in fast-moving contexts, responding to shifting community priorities, seasonal programs, and grant-funded initiatives which makes flexibility a top priority. To support these dynamic requirements, Object First also offers a consumption-based model that allows agencies to pay monthly for only the backup capacity they use.

This pay-as-you-use model provides predictable billing and scales effortlessly from 10 TB to 7 PB. As usage grows, the cost per terabyte decreases. Object First handles hardware refreshes, software updates, support, and optimization, eliminating lifecycle management burdens and procurement delays.

This model perfectly satisfies the financial and operational requirements of SLED agencies by enabling rapid deployment without the typical procurement delays or lifecycle management burdens. Agencies can start small, such as a school district adding new campuses or a municipality expanding public safety operations, and scale seamlessly as data storage needs grow, all while maintaining predictable costs and avoiding large upfront investments.

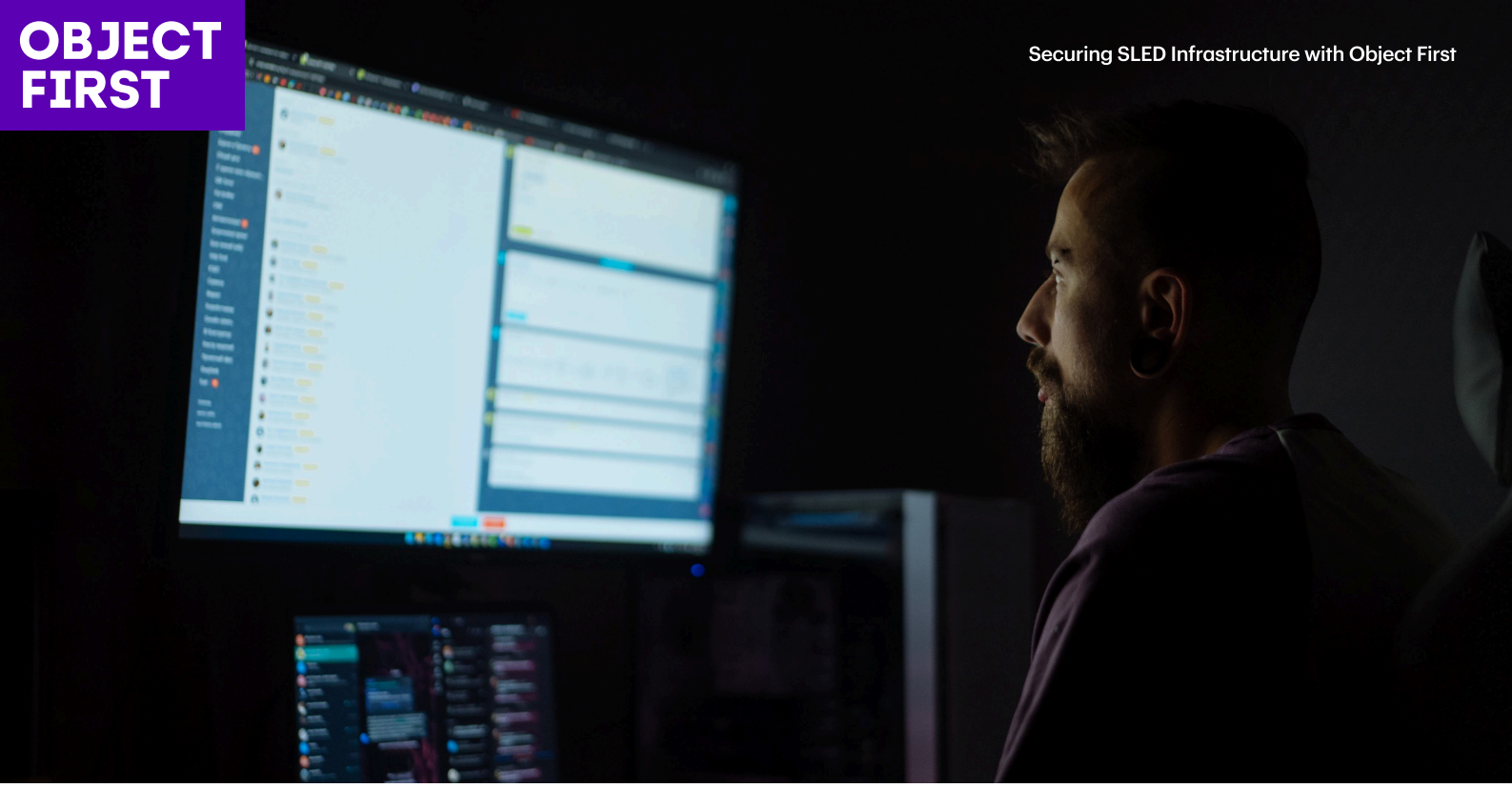


Ransomware resilience in SLED: unifying security, compliance, and recovery

State, Local, and Education (SLED) IT environments are naturally high-risk by nature. Administrators manage systems containing sensitive data, including criminal records, student information, and health data, under strict regulatory oversight. These systems must be secured against external threats, misconfigurations, and insider risk, while maintaining compliance with CJIS, FERPA, ADA, and state privacy laws.

Most SLED IT teams operate with limited resources. Staff often manage dozens of systems across hybrid environments, leaving little time for audits or policy enforcement. Security tools must be lightweight and simple since complex configurations increase the risk of mistakes.

A failed restore can delay emergency response, disrupt student services, or halt permit processing. A prime example occurred in Atlanta in 2018, when a ransomware attack crippled the city's computer systems, ultimately costing SLED leaders $2.6 million to recover from what began as a $52,000 ransom demand. The attack was ultimately attributed to "SamSam Ransomware," which performed the attack by infecting 3,789 servers and workstations, encrypting all files, and locking all computers.



Ransomware is targeting your backups

Legacy environments are ill-equipped to withstand modern ransomware threats. Attackers now target backup data directly, and without immutability or architectural separation between backup software and storage, ransomware can spread through backup environments, eliminating any viable recovery path after the dust has settled.

RTOs and RPOs are slipping out of reach

Compounding the issue, administrators are expected to meet stringent Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). However, legacy systems and fragmented infrastructure often lack automation and real-time replication. This forces reliance on slow, error-prone manual processes, making it increasingly difficult to achieve these targets, especially under pressure.

Cybersecurity controls aren't enough

Standard cybersecurity controls such as role-based access, multi-factor authentication, vulnerability scanning, and patching offer a baseline defense. However, they fall short of addressing the full scope of ransomware risks. In many SLED organizations, backup infrastructure and broader cybersecurity practices are deprioritized, creating blind spots that attackers are quick to exploit.

Access integrity is the weakest link

When backups reside on legacy systems, writable media, or exposed cloud buckets, they become prime targets. These setups often hinge on administrative access controls. If those permissions are compromised, the entire backup infrastructure is at risk. No matter how advanced a system may appear, its resilience is defined by the integrity of its access controls.

Object First contribution: Absolute Immutability by design

The Object First appliance ensures ransomware resilience and Absolute Immutability by design through WORM (Write Once, Read Many) principles and S3 object storage. Once backup data is written, it cannot be altered or deleted—even by compromised admin credentials—enforcing our Zero Access policy, which blocks all destructive actions regardless of user, credential, or API.

The Object First appliance also segments backup software from backup storage. This limits the blast radius of an attack: even if the backup application is compromised, the data remains protected.

With native Veeam integration, Object First simplifies deployment and eliminates the need for cloud tiering or object storage expertise. Backups are encrypted by default using AES 256-bit encryption provided by Veeam, supporting compliance with CJIS, FERPA, and state-level mandates.

For SLED teams, Object First delivers ransomware resilience without operational complexity. It enables fast, reliable restores and helps agencies meet RTOs and RPOs with confidence, even under active threat.

Object First: your ultimate defense against ransomware

When ransomware strikes, the future of your business hangs in the balance. In that moment, recovery matters most—getting back up and running as fast as possible, without unwanted complexity. Everything depends on how you decide to approach data resilience.

We make resilience simple with immutable backup storage that's purpose-built for Veeam. When your business, reputation, and career are on the line, Object First is your ultimate defense against ransomware.

Object First is built on Zero Trust best practices and is third-party tested to be secure, is simple to deploy and manage with no security expertise required and is powerful enough to supercharge Instant Recovery and scale with your business.

When your backup storage is this secure, simple, and powerful, you and your organization can become Simply Resilient.

Ready to see how SLED agencies are achieving uncompromising cyber resilience with absolutely immutable backups? **Request a demo today** to experience the difference firsthand.

OBJECT FIRST

Simply Resilient for Veeam