SOLIX™
Empowering the Data-driven Enterprise

E-BOOK

From Liability to Leverage: Quantifying ROI Through Solix Application Retirement

Risk Curve & Urgency: Why Retirement Can’t Wait

Part 1

www.solix.com

+1.888.467.6549

1. Executive Summary

Let’s be real: your legacy apps aren’t just outdated—they’re expensive, risky, and slowing your business down. Picture this: You're the CTO of a Fortune 500 company, and you just discovered that 40% of your IT budget goes toward maintaining applications that barely anyone uses. Sound familiar? You're not alone. Application retirement is the antidote. It means safely decommissioning old apps while retaining access to historical data.
The result? Lower costs, better compliance, and a boost in performance.

The ROI benefits are substantial: 30-80% cost savings, improved compliance posture, and dramatically enhanced system performance. Organizations are discovering that retiring legacy applications isn't just about cutting costs—it's about freeing up resources for innovation, reducing security risks, and accelerating digital transformation initiatives.

Solix Technologies offers a proven solution to make this transition smooth and measurable, delivering ROI through cost savings, compliance, and operational efficiency. This two-part series will show precisely how Solix Application Retirement turns your legacy liability into competitive leverage across every stage of the transformation journey. You'll learn proven methodologies, see real ROI calculations, and discover why leading enterprises make application retirement a cornerstone of their modernization strategy. By the end, you'll have the framework and confidence to build a compelling business case that gets executive buy-in. And we promise: no jargon, no filler: just practical insights and real numbers.

Your Complete two-Part Journey:

Part 1: "Risk Curve & Urgency: Why Retirement Can’t Wait”, exposes the shocking financial reality most organizations don't realize they're facing. You'll discover how legacy applications create exponential cost growth from $100K to $1.56M over just 10 years, why 65% of enterprises struggle with legacy sprawl, and how technical debt systematically undermines competitive advantage. This foundational knowledge is absolutely critical—without understanding the true scope of legacy costs (visible, hidden, and strategic), any retirement strategy becomes merely a technical exercise rather than a business transformation.

Part 2: Building on Part 1’s urgency, Part 2 turns narrative into numbers, “The Business Case & Self-Funding Execution with Solix”. Use an ALM governance lens (business value × technical health), build a defensible cost–benefit and NPV model, run multi-year ROI and break-even, and convert results into stakeholder KPIs. We break down savings across storage/infrastructure, licensing, compliance/risk, and operational efficiency so Finance, Risk, and IT align on one truth. Then operationalize it: customer proofs, portfolio-based selection, phased decommissioning, program governance, and a repeatable, self-financing rhythm—closing with the Strategic Case as a modernization flywheel.

2. Introduction to Application Retirement

Have you ever wondered how many applications your organization is running? Chances are, it's more than you think. Over time, businesses accumulate software like clutter in a garage—some apps are critical, but others are relics from a bygone era.

This legacy application sprawl eats up resources, increases risks, and slows down your ability to adapt. According to McKinsey 2024, 70% of IT budgets are spent maintaining existing systems, leaving little for digital transformation [1]. A Forrester survey revealed that nearly 60% of financial services CTOs believe their legacy tech stack is too expensive and inadequate for modern applications [2]. This isn't just inefficient—it's dangerous.

2.1. What Application Retirement Is and Isn't ?

Application retirement isn’t about simply deleting data or shutting down legacy systems without a plan—it’s a strategic process of decommissioning outdated applications while ensuring their data remains accessible, compliant, and secure. The goal is to archive historical data in a searchable, cost-effective format that meets regulatory requirements like GDPR, HIPAA, or SOX, and can be retrieved when needed for audits, legal inquiries, or analytics. It involves turning off the application and its infrastructure, migrating data to an easily accessible, compliant archive, and reallocating IT resources and budget toward more modern initiatives. It’s not a substitute for backups, nor just about moving data to cold storage—it’s about long-term data stewardship with the added benefit of saving costs and freeing up valuable IT capacity. To cut a long story short, **it’s not deletion; it’s optimization.**

2.3. The Stats Don't Lie

Here's a sobering statistic: IT organizations worldwide are burdened by an estimated $1.52 trillion in technical debt [3]. However, the human cost is even more staggering, with productivity loss, talent attrition, and loss of innovation time. Gartner predicts that by 2025, 75% of enterprise-generated data will be processed at the edge, rather than in traditional centralized data centers— an increase from under 10% in 2019 [4] - meaning, legacy applications built for centralized data centers will quickly become obsolete, costly, and risky. You’re not alone in this struggle.

According to a 2023 study, over 65% of enterprise applications are legacy systems, and companies spend 60-80% of their IT budgets maintaining them [5]. Another report says that by the end of 2025, businesses that delay modernization may spend up to 40% of their IT budgets just maintaining outdated systems [6]. This technical debt has serious consequences: employees lose up to 20% of their productivity working around inefficient tools, cybersecurity vulnerabilities increase (with average breach costs reaching INR 411.78 million globally in 2024), and growth potential is lost. In contrast, companies that embraced modernization in recent years experienced a 43% boost in efficiency and captured 31% more market share [7].

Beyond the expenses mentioned above, integration challenges often lead to isolated data systems that hinder analytics and obstruct efforts to build a comprehensive view of the customer. As per MuleSoft’s 2023 Connectivity Benchmark Report, companies invest around $3.5 million yearly on custom integration projects, with nearly 65% of that cost tied to connecting legacy systems.

The statistics tell a clear story: Organizations that don't actively manage application retirement aren't just missing opportunities—they're accumulating risks that compound exponentially over time.

3. The Cost of Doing Nothing

Picture this: Sarah, the CIO of a mid-sized financial services company, just got the quarterly IT spending report. Her legacy applications systems, which haven't been updated since Obama's first term, consume $2.3 million annually. That money could fund her entire digital transformation initiative, but instead, it's disappearing into the black hole of technical debt.

Sound familiar? Sarah's story isn't unique. Across industries, legacy applications have become the equivalent of paying rent on houses you don't live in anymore. Let me tell you about a healthcare organization we worked with last year. They had 247 applications in their portfolio. Sounds reasonable, right? Here's the kicker: 89 of those applications had fewer than 10 active users. One application—a patient scheduling system—cost $180,000 annually to maintain and was used by exactly three people.

Every dollar spent maintaining obsolete applications is a dollar not invested in cloud migration, AI initiatives, or customer experience improvements. Every developer debugging 15-year-old code is a developer not building the future. The costs associated with legacy applications can be broken down into three categories that’ll make any CFO’s eye twitch.

- ☑ **Visible costs** hit your budget like a sledgehammer: storage that grows 30% annually, maintenance contracts that increase 10-15% yearly, and infrastructure that costs more to keep running than replace. One aerospace manufacturer spent $40 million annually to keep their legacy inventory systems breathing.
- ☑ **Hidden costs** are the silent killers: security patches that take weeks instead of hours, audit preparations that consume entire quarters, and productivity losses that compound year after year. These don't show up on budget line items, but they erode your competitive advantage systematically.
- ☑ **Strategic impact** is where the real damage occurs: while you're babysitting legacy systems, your competitors are deploying cloud-native solutions that scale automatically, integrate seamlessly, and adapt to market changes in real-time.

3.1. Infrastructure, Storage, Maintenance Costs

Let's talk about the expenses that show up on your budget reports—the ones that make CFOs ask uncomfortable questions during quarterly reviews.

- **Storage Costs:** Storage costs follow a predictable but painful pattern. Legacy applications generate data like teenagers generate dirty laundry—constantly and without consideration for space constraints. A typical enterprise application creates 15-25% more data annually, but legacy systems lack the intelligence to distinguish between valuable information and digital junk.

  Here's the math that'll keep you up at night: If you're storing 100TB of legacy data at $0.12 per GB monthly, you're paying $12,000 monthly just for storage. But legacy systems don't compress well, don't deduplicate efficiently, and require multiple backup copies. That same 100TB likely costs you $35,000-45,000 monthly when you factor in redundancy, backup, and compliance requirements.

- **Maintenance Overhead:** The maintenance costs are compounded, like credit card debt. Industry data shows legacy application maintenance increases 10-15% annually[7], but that's just the beginning. As systems age, they demand specialized consultants—often charging 35–45% above market rates due to scarce expertise in COBOL and outdated databases—along with costly extended support contracts from vendors aware of your dependency, and custom security patches to address vulnerabilities that standard solutions can’t fix.

- **Infrastructure Dependencies:** Infrastructure costs create a particularly cruel trap. Legacy applications were designed for dedicated hardware in on-premises data centers. They can't take advantage of cloud economics, auto-scaling, or modern virtualization. The result? You're paying premium prices for deprecated hardware while your competitors run similar workloads for a fraction of the cost.

- One North American life insurance company discovered, that they were spending 60% more on infrastructure than necessary. Its mainframe-based applications required specialized hardware, dedicated cooling, and round-the-clock monitoring. With **Solix Application Retirement**, its infrastructure costs dropped by 60% while actually improving performance and reliability.

Category	Small Enterprise	Medium Enterprise	Large Enterprise
Application & DB Servers	$10,000 – $20,000	$25,000 – $40,000	$60,000 – $100,000
Storage (SAN/NAS)	$5,000 – $10,000	$10,000 – $20,000	$40,000 – $70,000
Backups / DR	$2,000 – $5,000	$5,000 – $10,000	$15,000 – $30,000
Hardware Support	$2,000 – $5,000	$5,000 – $15,000	$20,000 – $40,000
Power, Rack, Cooling	$2,000 – $5,000	$5,000 – $10,000	$15,000 – $25,000
Network Equipment	$1,000–$3,000	$3,000–$7,000	$10,000–$20,000
Security Appliances	$1,000–$3,000	$3,000–$7,000	$10,000–$20,000
Monitoring/Management	$1,000–$2,000	$3,000–$7,000	$4,000–$10,000
Total	**$28,000–$63,000**	**$3,000–$7,000**	**$189,000–$355,000**

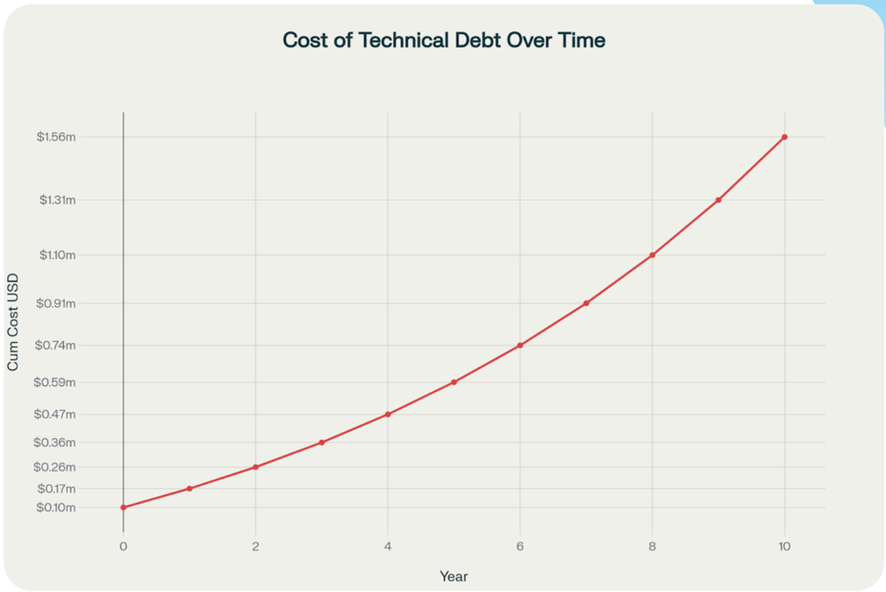
Table 1

Let’s look at a real-world scenario, estimating the average hardware and storage costs for a Tier-1 ERP vendor’s e-business suite deployment. The deployment involves a mix of server infrastructure, storage arrays, backup systems, and maintenance. While the exact numbers can vary based on deployment size, here’s a generalized estimate running on-premises:

Cost of Technical Debt Over Time

The cost of technical debt is sneaky—it starts small, then balloons as you pile on patches, storage, and maintenance for outdated apps. Let’s visualize how these expenses rise sharply over time and discover why early action can save a fortune.

Insight: Technical debt isn't linear—it's exponential. The graph shows an exponential growth from $100K to $1.56M over 10 years. OpEx grows at 15% annually, and risk costs compound at 12% annually due to increasing complexity and diminishing vendor support. What starts as $100K in annual costs becomes $1.56 million over ten years, with the acceleration becoming more pronounced each year as systems become more complex to maintain and more expensive to support.



Formula: TCO = CapEx + OpEx + Risk Costs

Graph 1

- *Capital Expenditure- Upfront or periodic investments in physical assets and long-term infrastructure needed to keep the legacy app running. It includes Hardware replacement/refresh cycles (servers, mainframes, network gear), Storage systems (SAN/NAS arrays, backup appliances), Software licenses purchased upfront (ERP modules, database licenses, middleware), Data center facilities upgrades (power, cooling, rack space), One-time migration or integration hardware (if expanding or interfacing with modern systems).
- *Operational Expenditure- Ongoing, recurring costs to operate and maintain the legacy application. This includes- Annual software maintenance & support feesExtended vendor support contracts (often at a premium for outdated software), Specialized consultant/contractor fees (COBOL, mainframe, outdated DB skills), Internal staff costs (time spent firefighting, patching, and supporting the old app), Custom security patches & compliance costs (since modern tools may not work), Energy costs (powering inefficient older hardware), Backup & disaster recovery costs, Downtime-related losses (if old systems fail more often).

3.2. Licensing & Support Overheads

If storage and maintenance costs are the visible wounds, licensing and compliance costs are the internal bleeding—often larger and more dangerous than what can be seen on the surface.

- **Software licensing:** Software licensing for legacy applications operates under what can only be described as "hostage economics." Once you're dependent on a legacy system, vendors know you have limited negotiating power. A 2022 Flexera survey found that 78% of companies with significant legacy footprints reported having minimal leverage with software vendors, resulting in license cost increases of 8-12% annually, well above inflation rates.

  The problem compounds when you consider that legacy applications often require multiple licenses, including the core application license—which typically increases annually, along with database licenses based on processing power or user count, integration middleware to connect with other systems, additional security add-ons to compensate for outdated protections, and backup and disaster recovery solutions to safeguard critical data.

- **Support Contracts:** Vendor support for legacy systems follows a predictable pattern: prices increase while service quality decreases. Support contracts become particularly expensive as applications age. While standard support might start at 15–20% of license fees, legacy systems often demand extended lifecycle support at a 25–40% premium, custom patches and fixes billed at hourly consulting rates, specialized expertise that commands premium pricing, and even emergency support contracts to address critical issues.

Let’s examine a real-world scenario for estimating the average licensing costs for the same Tier-1 ERP vendor’s e-business suite deployment. These costs include the base application, additional functional modules, database licensing, user access fees, annual support, one-time implementation expenses, and ongoing administration. While the exact figures vary based on deployment size, the table below provides a generalized on-premises estimate for small, medium, and large implementations.

Category	Typical range (small)	Typical range (medium)	Typical range (Large)	Note
Base EBS Application Suite	$100K – $200K	$300K – $600K	$1M – $2M	Pepectual includes core financials, supply chain, and HR
Additional Modules	$10K – $50K/module	$40K – $150K+	$150K – $300K+	Often priced per module, per user, or usage volume
Database Licensing	$35K – $60K (SE2)	$96K – $190K (EE)	$200K – $1.2M+ (EE)	EE: $47,500/processor CPUs common
User License	$800 – $4,000/User	$2,000 – $3,500/User	$3,000 – $3,700/User	Named/concurrent user or By the revenue license model
Annual Support/Maintenance	22% (22% of Total License Value)	22% (22% of Total License Value)	22% (22% of Total License Value)	Required to receive patches, updates, and support
Implementation (one-time)	$75K – $200K	$200K – $800K	$800K – $2M+	May include SI, Internal labour, and training
Ongoing Admin/Upgrade/Ops	$15K – $35K	$50K – $175K	$250K – $600K	DBA, updates, performance, security

Table 2

(Total License Value: A one-time (perpetual) purchase cost covering the organization’s right to use the ERP suite, including the base application, additional modules, database licenses, user licenses, and any optional add-ons or technology packs. It represents the organization's total "capital investment" in ERP licensing (i.e., the up-front spend spread over a 5-year useful life for ROI/TCO comparison).

3.3. Audit Exposure & Productivity Loss

Now let’s step into the danger zone—the costs that don't show up on quarterly reports but can destroy companies overnight.

- **Audit Nightmares:** Audit exposure creates its own category of expense and risk. Legacy applications may sit quietly in the background, but when an audit arrives, they can quickly turn into a liability. Historical data trapped in outdated systems often lacks consistent formatting, metadata, or proper access controls, making it difficult to extract and validate. IT and compliance teams scramble to piece together fragmented records from clunky interfaces, slowing audit readiness and increasing the risk of errors. What should be a straightforward process becomes a fire drill, consuming valuable time and exposing the organization to regulatory penalties.

- **Productivity Drain:** Even inactive or low-use legacy applications quietly erode productivity. Historical data locked inside them is slow and messy to retrieve, forcing employees to spend extra time validating records instead of focusing on higher-value work. IT teams also carry the burden of maintaining these obsolete systems—renewing licenses, troubleshooting outages, and keeping infrastructure alive long after its prime. Beyond that, critical workflows stall when important data remains siloed, making it impossible to automate or modernize processes fully. And when leaders need quick access to historical insights, these dormant systems introduce delays that slow decision-making across the business. This isn’t just inefficiency—it’s a hidden drag on your most valuable resource: human capital.

3.4. Impact on Digital Transformation & Business Agility

Legacy systems don't just consume resources—they actively sabotage your ability to compete in digital markets. It's like trying to race a Formula 1 car while towing a trailer full of anvils. Legacy systems dominate as the primary obstacle (50%)— outpacing the next major challenge (organizational structure at 38%) by a wide margin [7]. This suggests that outdated technology is a foundational blocker, likely impacting other areas like agility, collaboration, and skill requirements.

- **Cloud Migration Roadblocks:** Legacy applications weren't designed for cloud environments. They assume dedicated hardware, persistent connections, and specific network configurations. The result? Cloud migrations that take 3x longer and cost 2x more than planned. Moving 60% or more of IT systems to the cloud can boost annual profits by around 11%, a gain rarely matched by on-premises setups [8].
- **Data Democratization Delays:** Data democratization is hindered when information remains locked in legacy silos. Modern businesses require real-time access to comprehensive data for effective decision-making, yet outdated systems create obstacles, including proprietary formats needing specialized tools, limited API access, batch processing instead of real-time updates, and incomplete or inaccurate metadata.
- **Innovation Velocity Impact:** Customer-centric innovation demands the rapid deployment of new features and services, but legacy systems impose significant constraints. These include limited integration with modern customer touchpoints, slow response times that harm user experience, inflexible business logic unable to adapt to evolving needs, and scalability limitations that hinder business growth.

3.5. Risk Exposure Over Time

Time isn't kind to legacy systems. Like old cars, they don't just become less efficient—they become increasingly risky to safeguard. The risk isn't static—it compounds. Every month you delay retirement, legacy systems accumulate additional risk vectors.

- **Security Vulnerabilities:** Legacy systems are security Swiss cheese. They were built in different threat environments with different security assumptions. These systems were built in an era when security was an afterthought rather than a foundation, leaving them without modern encryption protocols, multi-factor authentication, real-time threat detection, automated security patching, or network segmentation support.

- **Data Breach Probability:** Cybersecurity threats evolve daily, but legacy systems remain frozen. Attack surfaces expand while defensive capabilities remain constant. The probability of successful attacks increases exponentially with system age. 80% of cyberattacks exploit vulnerabilities three years old or older, making legacy systems prime targets [9]. The financial impact is staggering. While the average data breach costs $4.45 million globally [10], breaches involving legacy systems are often even more expensive, as they are harder to detect quickly, typically involve more sensitive data, require specialized expertise for recovery, and may incur significant regulatory penalties.

- **Regulations and Penalties:** Every legacy system adds compliance complexity. Modern regulations like GDPR, HIPAA, and SOX assume you can quickly locate, report on, and manage data. Legacy systems make this nearly impossible without significant manual effort. Different systems store data differently, implement security differently, and handle audits differently. The result? Compliance costs that scale non-linearly with system count. Adding the 50th system to your portfolio might cost 10x more in compliance overhead than adding the 10th system.

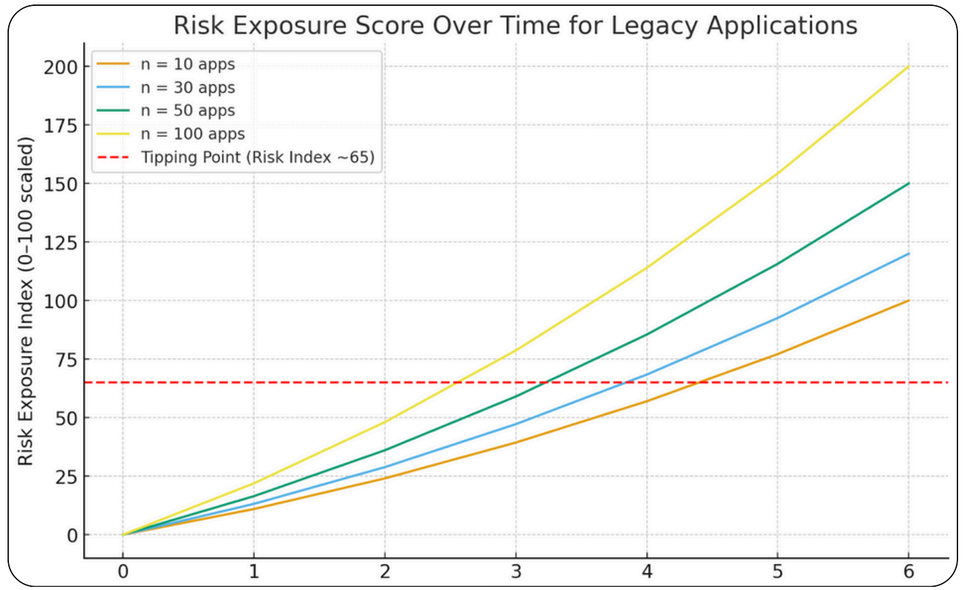
  The hidden multiplier effect arises when maintaining compliance with multiple regulations simultaneously, as each legacy system demands separate assessments, custom controls, and specialized reporting. For example, a healthcare organization spent $2.3 million annually on HIPAA compliance for its legacy systems, with each audit requiring weeks of manual data gathering, custom reporting, and specialized consulting. After implementing Solix Enterprise Archiving, their compliance costs dropped to $180,000—a 92% reduction.

Risk Score Over Time

Risk is like a snowball rolling down a hill. It doesn't just sit still — it compounds. A legacy system left in place may feel manageable at first, but every passing year adds another layer of vulnerability. Missed security patches, outdated compliance standards, and increasingly fragile infrastructure build on top of each other, accelerating the exposure curve. What begins as a small problem soon grows into a tipping point, where the cost and effort to contain risk far outweigh simply retiring the system. The chart below illustrates how risk escalates over time until it reaches a level no organization can realistically sustain.

Risk Exposure Score Over Time — This score starts near zero at Year 0, when systems are still supported and monitored, and rises steadily over six years. Security Risk increases linearly as patches lapse, Compliance Risk compounds exponentially as regulations outpace controls, and Operational Risk accelerates polynomially as infrastructure and expertise age. By Year 4, the index crosses a tipping point (~65) where managing risk becomes disproportionately expensive and disruptive.

Insight: Risk exposure doesn't grow evenly — it compounds. At first it seems manageable, but over time, overlapping security, compliance, and operational pressures push the system past a tipping point where legacy systems become a liability too costly to sustain.



Graph 2

Formula: Risk Exposure Index (0–100) = (Security Risk + Compliance Risk + Operational Risk) ÷ Maximum Total Risk × 100

Conclusion: The Exponential Time Bomb

You've now witnessed the brutal mathematics of legacy application sprawl—a financial and strategic crisis hiding in plain sight across enterprise IT portfolios. The evidence is overwhelming: 70% of IT budgets disappearing into systems that barely contribute to business value, while technical debt compounds exponentially from $100,000 to $1.56 million over just ten years. Infrastructure costs spiral 60% above necessary levels, maintenance overhead increases 10-15% yearly, and hidden productivity drains consume up to 20% of employee effectiveness as workers navigate antiquated interfaces and fragmented data silos. Meanwhile, security vulnerabilities turn legacy systems into prime targets for the 80% of cyberattacks that exploit vulnerabilities three years old or older.

The Risk Exposure Over Time analysis reveals the most terrifying pattern: risk doesn't grow linearly—it compounds like credit card debt. By Year 4, the Risk Exposure Index crosses a critical tipping point at 65% where managing risk becomes disproportionately expensive and disruptive. What begins as manageable maintenance transforms into crisis management, with overlapping security, compliance, and operational pressures pushing systems past sustainable thresholds. A healthcare organization discovered this harsh reality when their HIPAA compliance costs reached $2.3 million annually for legacy systems, while competitors using modern platforms achieved the same compliance outcomes for under $200,000—a 92% cost differential that compounds year after year.

Perhaps most devastating is how legacy systems actively sabotage digital transformation initiatives. With 50% of enterprises citing legacy applications as their primary modernization obstacle, these systems don't just consume resources—they prevent strategic repositioning. Cloud migration projects take 3x longer and cost 2x more when legacy dependencies create architectural roadblocks, while innovation velocity suffers as organizations find themselves racing Formula 1 cars while towing trailers full of anvils. Every month of delay multiplies both the problem's severity and the solution's urgency, with legacy costs rising 10% annually meaning $700,000 in annual waste becomes $1.13 million by Year 5.

The next installment reveals how leading enterprises convert these mounting liabilities into revenue-positive strategies. You'll discover the mathematical frameworks that convinced CFOs to approve millions in retirement projects, delivering documented returns like 697% first-year ROI and $1.6 million in net value over three years. Global case studies show how systematic retirement creates self-funding cycles where each application retired generates resources to accelerate additional retirements, transforming organizations from spending 70% of IT budgets maintaining digital museums to investing that capital in AI, automation, and customer experience innovations. The question isn't whether legacy systems are destroying value—the evidence is mathematical and irrefutable. The question is whether you'll master the proven frameworks that turn your biggest liabilities into transformation funding.

SOLIX™
Empowering the Data-driven Enterprise

Stay Connected

www.solix.com

info@solix.com

+1.888.467.6549