



Software-Defined Storage: Enabling Digital Transformation Through Efficiency, Security, and Compliance

Executive Summary

Digital transformation (DX) is now an organizational imperative across every vertical, geography, and segment. Over the next few years, businesses that fail to invest in transformative technologies will fall behind their contemporaries or fail entirely, while public sector organizations risk failing to uphold their mandates to provide the services their constituents require. Leading organizations are already making investments in DX technologies, from mobility and cloud to the Internet of Things (IoT), cognitive computing, and AI.

The goals of DX may vary, as do the forms it takes, but one constant of digitalization is data — the fuel that drives the engines of transformation. As the amount of data organizations create continues to expand at 30%–50% per year, the demands we make on this data also increase. We require scale and performance unheard of a decade ago, our applications reside within our own datacentres as well as our partners' or the cloud, and the risks associated with our data in terms of security, data protection, and regulatory compliance continue to grow. A further stress on the system is the emphasis from line of business for IT to provide this capacity and these capabilities with greater efficiency and agility than traditional procurement can provide. Organizations find it difficult to predict their technology requirements three to five years out, but expect IT to be able to react to changes in business strategy with speed and flexibility — capital expenditures with four- to five-year life cycles cannot meet these business imperatives.

Software-defined storage (SDS) aims to address these challenges through a new paradigm in storage deployment and data management. x86 servers provide a lower cost environment than traditional storage arrays, with the ability to scale, manage, and support advanced virtualization capabilities through easily updated software rather than custom fabricated ASICs. Capacity can be addressed wherever the network extends, from the endpoint to the datacentre to the cloud.

Organizations investing in SDS will be well positioned to take advantage of the scale, efficiency, security, and compliance services that software-focused, evergreen infrastructure can provide to next-generation datacentres.

Organizations that deployed SDS found that benefits achieved exceeded every expected benefit, on average.

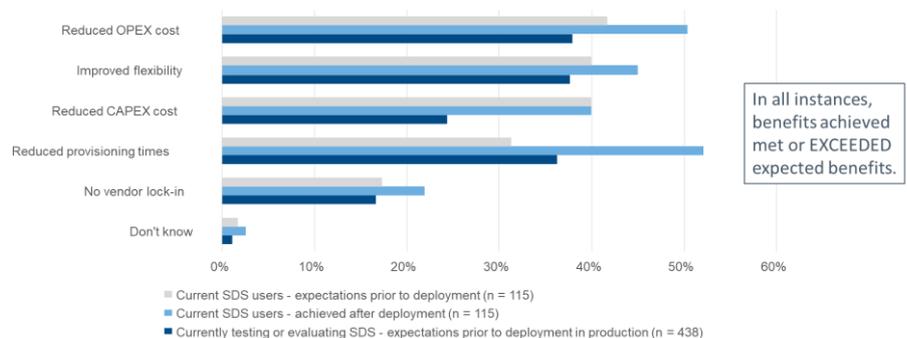
SDS Adoption: Efficiency is the First Hallmark of the Software-Defined Datacentre

The most easily recognized benefit and key motivator for many organizations adopting SDS is efficiency. Reducing capital and operational expenditures, increasing utilization, and simplifying management of storage resources are easily defined and measurable benefits of these sorts of implementations, and they are some of the very same benefits many organizations have realized in the past decades through consolidation, virtualization, and cloud adoption. Figure 1 shows that 3 of the top 5 drivers for SDS adoption have to do with cost-effectiveness and efficiency.

Figure 1
Benefits Expected and Achieved by SDS Adopters

Key benefits of SDS deployment

Cost is a major driver for SDS deployment, provisioning times an unexpected benefit



Source: IDC, 2017

Most new technology deployments are a mixed bag of over- and under-delivering on promised or expected benefits. SDS bucks this trend, where each of the top 5 benefits driving SDS adoption met or exceeded respondents' expectations. This surprising result is a strong indicator that investments in SDS will help IT achieve their tactical goals in service of DX; that is to say "do more, with less."

SDS Adoption: Agility and Flexibility Are Next-Level Goals; Security is Now Table Stakes

Businesses continue to expect and demand agility and speed from their IT departments. IDC surveyed over 200 North American enterprises and found that through 2020, increasing overall business agility was considered to be the top IT imperative by 59% of respondents. In second place came improving security and compliance.

The most unexpected benefit of SDS shown in Figure 1 was the reduction in provisioning times for respondents that had implemented SDS. This is one key way IT departments can help development teams shorten application delivery cycles, along with the ability to move workloads seamlessly between development, test, and production environments including traditional datacentre infrastructure,

converged and hyperconverged, and cloud deployments. Virtualization and abstraction of data and metadata is key to separating applications from silos, and is yet another way SDS helps IT meet line of business' goals.

Data security is obviously a hot topic among organizations of all shapes and sizes today, with intrusions, data breaches, cryptographic ransomware, and misuses of personal and financial data making the news daily. The ability to move workloads to their ideal infrastructure has provided enterprises with a tremendous amount of value, but at the same time it has completely changed the security landscape for organizations.

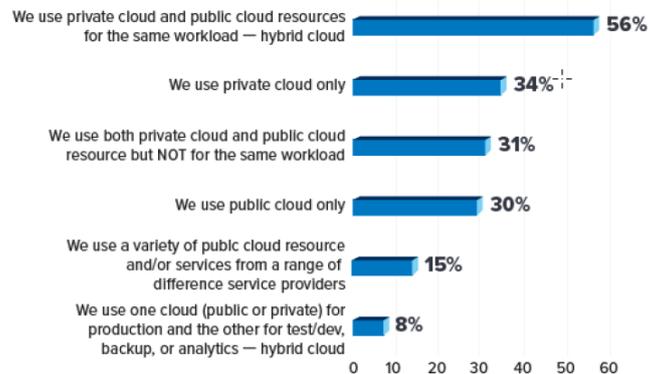
The amount of high-value data moving from the datacentre to the cloud or to end-user or edge devices is growing exponentially, leading to motivations for increased investment and sophistication within the cybercriminal world. The number of devices and environments has grown similarly, meaning the number of attack surfaces has grown as the perimeter dissolves. And finally, the number of security toolsets has grown, making it impossible for all security personnel to be qualified to deal with every form of threat. Point solutions typically work for a particular workload, or against a particular threat.

Understanding that breaches are going to happen, storage administrators are well advised to ensure that what is taken is unusable, by advanced cryptographic methods as well as data segmentation and separation. Incomplete sets of unintelligible data should be the only payload an intruder has access to, and data protection and recovery via proper replication and backup technologies across multiple geographies, storage deployments, and media are essential to peace of mind for an organization.

SDS Adoption: Hybrid, Multicloud Environments With Full Automation Are the End Game

IDC believes that no single deployment methodology can fulfil the requirements of all workloads for all end users. The performance, scale, connectivity, and usage of the growing application ecosystem means that infrastructure must vary, SLAs must vary, governance monitored, security postures updated, etc. The ability to move workloads from on-premise to private cloud to public cloud and within clouds for different phases of the data life cycle is critical to maximizing value and return on technology investments. Companies we've surveyed agree — over half of our survey respondents favour a multicloud approach for even single workloads.

Figure 2
Over Half of Respondents Use Hybrid Cloud



Source: IDC, November 2017

The opportunity to fine-tune infrastructure to the needs of applications, and derive maximum value from organizational data, brings with it risks to the organization. SDS helps ameliorate some of these issues, especially when it comes to managing architectures, as the virtualized nature of the data typically aids in platform agnosticism. As well, maintaining a separate control plane can aid in providing an enterprisewide view of data throughout its life cycle, which facilitates DPRS and backup, archive, governance, compliance, and even security.

Essential Guidance

CIOs need a plan to migrate their organizations to a software-defined world. It's coming, and it's accelerating the drive toward digital transformation. The risks faced by first movers in new technological territories are far less threatening than those laggards are bound to experience.

Evaluating which lines of business stand to gain the most from the benefits that SDS can bring to their data is a critical first step down this path. Our mantra has always been "the right data in the right place at the right time," meaning that clients' data must follow the workloads. The key first steps in a transformation will be evaluating risk, returns, costs and benefits, whether an organization is facing granular decisions about media types and storage mechanisms, or enterprisewide data protection plans, information life-cycle management, and data governance.

CIOs must be proactive in explaining the benefits of new technologies such as SDS, hybrid cloud deployments, and end-to-end encryption to senior line-of-business executives, including operations and finance. Technology for technology's sake, or "shiny object syndrome," is not the reason for investment. Accelerating digitalization, reducing development life cycles, defending against data breaches, increasing agility, increasing datacentre efficiency, and reducing vendor lock-in are.

When a migration plan is in place, investing in the right people, whether they are internal to your organization, new hires, or part of the vendor and partner community, will be key to unlocking the value in the software-defined datacentre. Enterprises have identified a lack of experience and skills with SDS as a roadblock

to implementation success. Developing, hiring, or partnering with vendors that have those skills and experience must be a top priority.

Leonovus Company and Product Profile

Founded in 2010 in Ottawa, Canada, Leonovus aims to be a world leader in providing ultra-secure, automation/orchestration of software-defined object-based storage to organizations at scale in a variety of segments and industries.

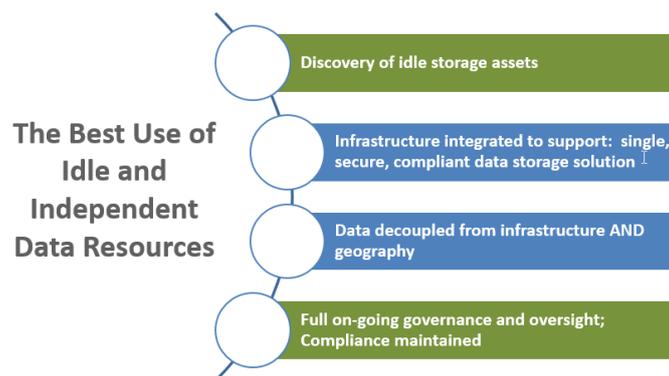
Leonovus has direct sales forces and channel partners in the United States and Canada to capitalize on its most recent release of Leonovus 3.0, currently in active production as well as trials with customers in a variety of verticals, including law enforcement and public safety, healthcare, and financial services. Four months of testing and evaluation with the Government of Canada led to Leonovus' certification and prequalification for the Build in Canada Program, designed to accelerate investment in innovative technology developed in Canada.

It recently hired Electronic Warfare Associates Inc. to advise it on its submission of FIPS 140-2 certification to the National Institute of Standards and Technology, which would make it one of the first companies with embedded blockchain security to have this certification, required for many governmental and heavily regulated industries disseminating sensitive information.

The three key precepts of efficiency, security, and compliance are at the heart of Leonovus' product offering:

- **Efficiency.** Greater utilization and efficiency across the enterprise is achieved through discovering and making use of any available capacity within the organization, including unused Microsoft OneDrive and Google Drive space. Any on-premise hardware and capacity, as well as any cloud environment, can be utilized, helping to avoid vendor lock-in.

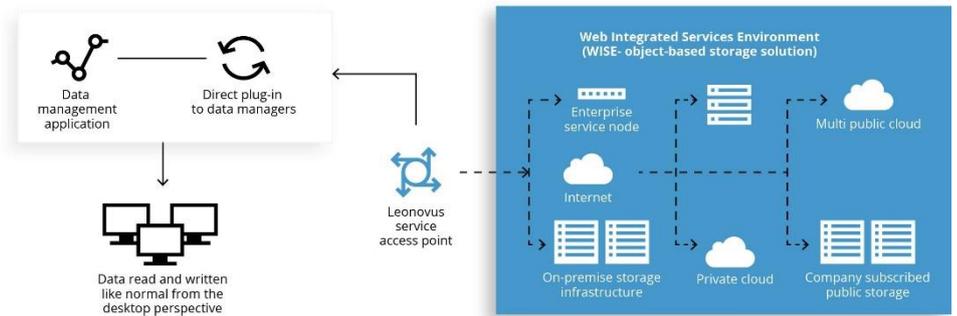
Figure 3
Efficiency



Source: Leonovus, 2018

- **Security.** Proprietary algorithms that slice, encrypt, and distribute files at flight and at rest assure clients that no data theft or security breach can lead to intruders gaining access to any usable data. Dual-path event tracking, digital signatures, and blockchain immutability ensure data remains tamper-proof.

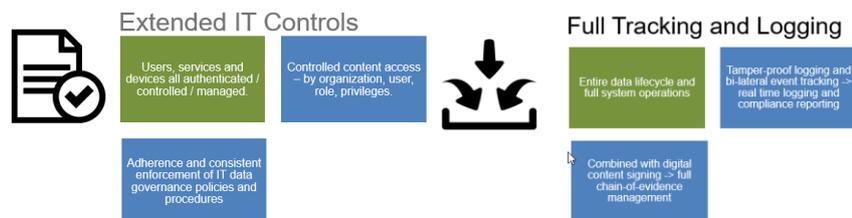
Figure 4
WISE Network



Source: Leonovus, 2018

- Compliance.** A single-pane-of-glass view of data across enterprise datacentres as well as throughout hybrid and multicloud environments provides visibility of the entirety of an organization's data. Full policy control with data classification for user, service, and device based access and management allows automated management across hybrid environments. And a fully auditable chain of custody tracked and logged by a blockchain hardened ledger ensures compliance and simplifies governance and risk management, proven to regulatory authorities by extensive reporting available within the system.

Figure 5
Single Management View



Source: Leonovus, 2018

Challenges and Opportunities

Leonovus faces many of the same challenges new entrants to the infrastructure software space face. Companies of all sizes are often more comfortable with "tried and true" solutions with a long history of successful implementations, and this is particularly true for the industries and segments most likely to benefit from Leonovus' offering: petabyte-scale implementations in large enterprises, financial services, public sector, healthcare, law enforcement, and public safety. Customers in verticals dealing with sensitive data tend to be conservative when introducing new storage technologies, requiring small-scale deployments to provide proof of execution. Prospective buyers facing rigorous regulatory oversight will often need

to hear from satisfied customers that have solved similar problems in order to accelerate the sales process.

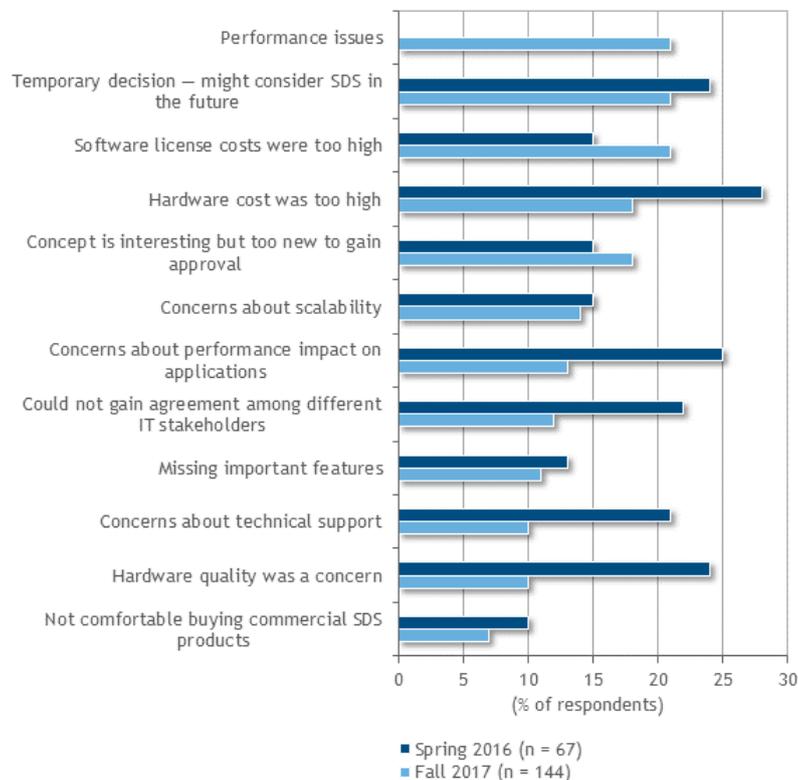
Demonstrating the value of Leonovus 3.0 will require Leonovus to prove that it is able to increase efficiencies by reclaiming unused space, as well as managing data governance with immutable proof of chain of custody as data moves throughout the hybrid cloud for full compliance with customer and industry regulations. These are non-trivial but manageable expectations. Proving the effectiveness of Leonovus' patented algorithms that break apart files, encrypt the resultant objects, and distribute them across multiple storage environments is absolutely key to their value proposition, and will require both government and industry certification as well as "time in the wild" to assure customers that their data is secure.

Compared to traditional external storage arrays, deployments of SDS for mission-critical applications is relatively new. Many of the key data services needed to effectively manage dense mixed enterprise workloads — such as snapshots, quality of service, and replication — have only been introduced onto SDS platforms over the past few years. This results in a dearth of both organizations and personnel with the expertise and experience to deploy SDS comfortably for key workloads.

However, between 2016 and 2017 IDC saw many of the impediments to SDS adoption becoming far less of an issue for our survey respondents, as seen in Figure 6.

Figure 6
Criteria for Avoiding or Terminating an SDS Implementation

Q. Why did you decide not to use (or stop using) SDS?



Source: IDC's Storage User Demand Study Survey, spring 2016 and fall 2017

Conclusion

The next few years will see the development of increasingly sophisticated storage services and mechanisms built on software, instead of the custom hardware that dominated the client-server era. Media of all types across the entire enterprise will be available "on demand" to storage services that are customized to meet any workload requirements. Our data will require the same mobility that applications demand; as compute shifts in and out of the traditional DC and between multiple clouds, so will our data and metadata follow.

The software-defined datacentre is one key to this digital transformation. Virtualization taught organizations the value of separating their workloads from the hardware they run on. IDC predicts that by the end of 2019, over 50% of enterprise IT infrastructure will have moved to the software-defined model. We also believe that hybrid traditional/cloud deployments will be the dominant modality during this period.

Due to the increasing movement of data through the borders of our datacentres, the traditional "firewall" paradigm of intrusion prevention and data protection will not be sufficient to secure data. Encryption of all data at rest and in flight, no matter whose infrastructure it is currently residing on, will become table stakes for storage providers, as will data governance policies and compliance tools to ensure and demonstrate the privacy and security of business and user data.

The software-defined model is also critical to the success of those endeavours. Security will become a proactive AI versus AI contest, and the ability to quickly and easily insert security, data protection, and compliance services into a software model in an automated fashion must become commonplace. While our data capacity and capabilities continue to grow exponentially, these trends will only heighten the disparity between technology resources and human resources. Skills and manpower shortages will ensure that organizations of all sizes must build the teams and seek the partners and tools that provide the intelligence required to deploy SDS successfully.

IDC CANADA

33 Yonge Street
Suite 420,
Toronto, ON M5E 1G4

Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions:

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701
USA P.508.872.8200
F.508.935.4015 www.idc.com.

Copyright 2018 IDC.
Reproduction is forbidden unless authorized. All rights reserved.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.