Working Smarter, Not Harder:
How Pre-Built AI, ML, and Automation Capabilities Boost Opportunities

July 2022

Author:
Archana Venkatraman

IDC #EUR149277522

An IDC InfoBrief, sponsored by
Businesses are entering a period of rapid change and are doubling down on digital investments

By 2023, one in two companies will generate more than 40% of its revenue from digital products and services, compared with one in three in 2020.

With 90% of organizations believing a digital-first strategy is essential for resilience and adaptability in an uncertain world, CEOs and other high-ranking senior executives are increasingly turning to digital technologies as the primary solution to overcome challenges and achieve business outcomes.

AI and analytics, SaaS experience, cloud-native technologies, and cloud migration — the four hot areas for tech investment

- **Accelerated rush to cloud**
  Cloud spend by 2025 will exceed 1.3 trillion, with a 16.9% compound annual growth rate.

- **Accelerated AI investments**
  AI revenues (including software, hardware, and services) are set to top $5 billion by 2024.

- **Cloud-native workload development**
  New production-grade, cloud-native apps will increase from 10% to 70% by 2024, thanks to microservices, containers, and DevOps advances.

- **SaaS-first and cloud-first operating model**
  SaaS applications will account for 59.6% of the cloud market in 2024 (up 14.6% from 2020).

By 2023, one in two companies will generate more than 40% of its revenue from digital products and services, compared with one in three in 2020.

With 90% of organizations believing a digital-first strategy is essential for resilience and adaptability in an uncertain world, CEOs and other high-ranking senior executives are increasingly turning to digital technologies as the primary solution to overcome challenges and achieve business outcomes.
There is a laser sharp focus on demonstrating ROI for digital investments, especially with data and operational resilience

With data becoming the currency of digital organizations, business outcomes such as resilience, data availability and protection, and optimized operations are becoming key metrics of digital investment success.

Data loss protection
By 2023, most high-ranking senior executives will implement business-critical KPIs tied to data availability, recovery, and stewardship as rising levels of cyberattacks expose the scale of data at risk.

Cloud economics
By 2025, 60% of enterprises will fund line-of-business and IT projects through opex budgets, with a focus on outcomes that are determined by SLAs and KPIs.

Cloud-based data protection
By 2025, 55% of organizations will have migrated their data protection systems to a cloud-centric model to centrally manage core, edge, and cloud data protection from the cloud.

Cross-cloud data governance
Seeking distributed data consistency, 75% of organizations will implement tools for multicloud data logistics by 2024, using abstracted policies for data capture, migration, security, and protection.

Data protection, governance, and security are becoming boardroom priorities. IDC expects public enterprises’ valuations to be based as much on confidence in data controls for effective use of data as on financial controls. This will increase focus on spend for data-centric solutions. How CIOs, CDOs, and CISOs ensure effective “controls” for data assets will be as important as how CFOs build financial controls.
The complexities and dynamism of IT make it harder for organizations to realize the value themselves, paving the way for next-gen service providers

The growing complexity of applications, infrastructure, and organizational constructs — such as DevOps, agile, and site reliability engineering (SRE) — and the use of hybrid cloud are challenging traditional approaches to IT operations and management.

The traditional approaches are slowing down organizations’ time to market, developer productivity, and overall IT resilience. This is forcing IT teams to explore strategic partnerships with service providers, so businesses can focus on their core competencies. C-suites realize that working more closely with industry ecosystem partners is necessary to spark innovation; augment skills, capacity, and knowledge; and enable resilience, according to IDC’s 2021 Future of Industry Ecosystems Global Survey.

To keep up with the scale of the operational challenge, MSPs can take greater advantage of policy-driven automation and intelligent AI/ML-driven operations to deliver secure, resilient, and autonomous environments to their customers. They can then offer a rich suite of services and be ready to capitalize on the opportunities — IDC predicts that by 2026, 90% of global 2000 CIOs will rely on AI- and ML-driven solutions for resilience, remediation, and workload strategies.

Well-informed MSPs are already considering this. According to IDC’s European Partner Survey 2021, 63% of MSPs are working with customers at a strategic level for digital transformation and are “co-creating with customers” to develop a mutually beneficial, bright digital future.
Three key areas where forward-thinking service providers can add value to organizations’ resilience strategies

**Digital infrastructure resilience and trust.**
In the next one to two years, organizations are likely to double down on efforts to ensure cyberattack recovery, robust and reliable backup, consistent application performance, ongoing infrastructure sustainability, and supply chain integrity. Organizations will carefully assess their strategic partners’ approaches to ensure data and infrastructure resilience.

**Data-driven operational complexity.**
In the next three years organizations will find that the volume and value of critical data, including edge-driven data creation and processing, are forcing significant application architecture and data stewardship changes, which in turn place new demands on digital infrastructure. Data protection, integration, analytics, and management will become top priorities. Organizations will invest in automation and analytics to ensure application performance and data protection and compliance, and to manage latency and ensure infrastructure scalability.

**Business-outcome driven sourcing and autonomous operations.**
In the next five to six years, digital infrastructure will be largely sourced, managed, and optimized using intelligent, policy-driven, self-driving, and self-healing automation, driven by application and workload-aware AI/ML analytics. A new generation of strategic partners will bring deep vertical market knowledge and business-focused expertise to ensure that organizations achieve the business outcomes expected. Next-generation infrastructure anchored by fit-for-purpose computing platforms will be optimized for advanced data management and analytics capabilities.

But service providers will need to revise their approach and update their platforms to capitalize on the value of automation and AI- and ML-driven intelligence that is embedded in the architecture.
Without next-gen platforms built with AI and automation, service providers can’t address the unprecedented data concerns created by a fragmented environment, at scale and speed.

Can’t manage what you can’t see: without next-gen platforms built with AI and automation, service providers can’t address the unprecedented data concerns created by a fragmented environment, at scale and speed.

Organizations fear data loss across their on-premises, hybrid cloud, SaaS, and container environments due to:

- Ransomware
- Accidental deletion
- Cloud platform outages
- Reliance on default retention
- Data corruption
- Lack of access to historical data

IDC’s 2021 European Multicloud Survey showed that 7 out of 10 organizations are already running many key applications on containers and cite security, data management, and recovery in these “new environments” as most challenging.

Data loss fears in SaaS environments is also a top concern.

Q. In which of the SaaS and PaaS environments currently in use in your organization are you most concerned about data loss and accidental deletion?

- Microsoft 365: 42%
- Oracle SaaS: 16.5%
- Google Workspace: 15.5%
- SAP SaaS: 15.4%
- Salesforce: 10.4%

Source: IDC’s European Multicloud Survey, 2021 (n = 925)
Shrewd MSPs are adopting the “rent before buy before build” mantra

Service providers need to balance engineering efforts, time to market, and revenue opportunities. IDC believes that MSPs that capitalize on platforms that have pre-built AI- and ML-driven intelligence can accelerate their time to market, help deliver strategic value to their customers, and grow revenue opportunities.

Service providers don’t need to build home-grown AI and ML services from scratch when they can leverage the existing intelligence built into next-gen cloud data management platforms to:

- Get instant visibility into data, applications, and SaaS instances in customers’ environments to identify potential risks, as well as compliance and resilience gaps
- Better detect malicious files or anomalies across hybrid environments
- Protect the full range of cloud, data, and applications
- Demonstrate the risks, via quick visualizations, to customers, especially as IT teams struggle to keep track of growing applications and data environments
- Highlight data environments that remain unprotected and improve the ability to seamlessly expand data protection services and policies to quickly accommodate newer environments
- Amplify the value of being continuously resilient, “always protected,” and “fully protected” without adversely affecting the speed a business can innovate
- Deliver consistent data services for hybrid cloud and robust SLAs around availability and data protection
- Avoid provisioning additional specialists and resources in the event of big restores
- Make business continuity and recovery a true differentiator

It took one managed services provider two years to build intelligent detection and recovery capabilities in-house with high investments in skilled professionals, IT resources, and engineering capabilities. The MSP is now evaluating how to cost-efficiently scale the in-house capabilities.

Another MSP adopted a platform vendor’s machine-learning model to demonstrate how its services can better detect and remove malware in backup data, so that customers can have safe recoveries. The AI capabilities available at the platform level helped the partner deliver intelligent data management services immediately and gain deeper visibility to identify newer opportunities.
Time to make use of AI/ML in cloud data management platforms as market demands soar

Alongside focused investment in digital building blocks and resilience, organizations’ technology objectives and strategies are changing too.

IDC’s 2021 Future Enterprise Resilience Survey showed that 61% of organizations are reducing the time and effort required to manage their technology investments and IT environments. A further 55% said they are aggressively shifting toward paying for technology investments based on consumption.

Businesses are increasing their reliance on service providers to ensure robust IT and data management services, so they can focus on their IP, overcome talent scarcity challenges, and build digital products and services confidently.

This year, IDC expects 40% of large enterprises’ IT budgets to be redistributed due to adoption of integrated as-a-service bundles in security, cloud platforms, virtual workspaces, and connectivity. In the next two to three years, digital-first enterprises will shift 70% of all tech and services spending to as-a-service and outcome-centric models.

Demand for these services is significant: IDC forecasts that the DPaaS market will grow at a 19% CAGR from 2021 to 2025, totaling $18.4 billion. This compares with just a 2.7% CAGR for “traditional” data replication and protection software solutions over the same period.

This provides new opportunities for MSPs with the intelligent and automation capabilities at their fingertips to meet customer expectations around cross-cloud workloads, governance, security, and data protection. For unprepared MSPs, the enterprise IT strategy trends are an existential risk.

Managed service providers need to raise their game to meet this challenge

It’s time to adopt the low-risk path and leverage modern capabilities such as cloud platforms, AIOps, ML, automation, policy engines, auto-scaling, and ediscovery to become relevant in the digital future. Becoming strategic and helping organizations boost their resilience can help MSPs become trusted partners as customer data and environments grow.
Demonstrate immediate business value by addressing acute business pain points and grow the business

IDC research shows that more than 90% of organizations have been attacked by malware/ransomware and more than 80% have fallen victim to a malware attack. According to IDC’s Future Enterprise Resilience Survey (FERS Wave 6, August 2021), 35% of organizations have experienced three to four incidents in the past 12 months alone. Of those impacted by ransomware, the consequences cited were significant. More than half (59%) of organizations in EMEA said they experienced business disruption of “a few days to a week” due to a recent ransomware incident.

Ransomware

In 2021, ransomware incidents affected some of the largest, highest-profile organizations with significant cybersecurity budgets:

- Ireland’s healthcare service suffered a ransomware attack with the Russia-based Conti gang demanding $20 million to restore services.
- Colonial Pipeline was forced to shut down an entire gasoline pipeline system and pay a $4.4 million ransom to hackers.
- JBS, the world’s biggest meat processor, paid an $11 million ransom after having to shut down operations in the U.S., Australia, and Canada.

Lack of control over dynamic environment

According to IDC’s 2021 Multicloud Survey, around 12% of organizations admitted that they “don’t know” what percentage of their applications run on containers. Using modern approaches such as AI-driven operations can provide a more holistic picture of the IT environment and identify applications and workloads that are not protected.
MSPs can do more with less using AI and ML

Attacks can't be prevented, but smart alerts, anomaly detection, and fast restores at scale can mitigate risks

Main data protection challenges

1. Ransomware protection
2. Data fragmentation
3. Spiraling costs of data management
4. SaaS data protection
5. Copy data management

MSP budgets are tight.

Using policy-driven automation and intelligent AI/ML-driven services can help mitigate cyber risks and data management challenges.

The ability to better analyze, integrate, and act on the insights is a necessity. The combined use of ML models with automated processes will enable faster response times, improved decision making, and an efficient model to deliver business outcomes. AI-based insights can improve service transparency and boost trust in the services.

MSPs cater to a wide range of customers across verticals, sizes, and complexities.

Having access to next-gen AI capabilities can open doors to new service opportunities.
Stand apart in a crowded market by making AI and ML the competitive differentiator

**ONE IN EVERY FOUR BUSINESS LEADERS**
cited SaaS data protection as a high priority for investment in the next 12 months.

23% believe that adding SaaS data protection can help boost their organization's data resilience.

An ML-driven approach to overcoming these fears can give MSPs a competitive edge.
Learning from the leaders: forward-thinking enterprises seek these five capabilities to develop a competitive edge

*MSPs leveraging automation and intelligence at the platform level are best placed to meet the following requirements at speed and scale:*

- **47%** Intelligent security and/or digital trust
- **43%** Access to integrated real-time (less than an hour old) data
- **40%** Right cloud strategy for the right workload
- **40%** Automation and orchestration
- **38%** Programmable infrastructure — software-defined storage (SDS), software-defined networking (SDN), serverless, containers, Kubernetes, etc.

*Source: IDC's Multicloud and Next-Generation Infrastructure Survey (n = 1,187)*
IDC recommendations

With an increase in ransomware attacks across all applications, the top priority for organizations is to minimize data loss. Cloud data management vendors committed to infusing AI and machine learning into their platforms can empower MSPs to deliver consistent data protection at scale, gain deeper insights to better protect customers’ data, and improve automated upsell opportunities.

MSPs have a golden opportunity to leverage intelligent cloud data management platforms and champion data governance, trust, and resilience to become strategic in their customers’ data-driven journeys.

IDC predicts that in the next two to three years 55% of organizations will have migrated their data protection systems to a cloud-centric model to centrally manage core, edge, and cloud data protection from the cloud. MSPs must act now to take advantage of this $18 billion+ market.

Without insights into data and workload protection, organizations are flying blind into their digital futures. MSPs can bring data to make the digital future secure, compliant, and resilient. They can empower their customers by identifying applications and workloads that are not protected. Around 12% of organizations, for example, admitted they don’t know what percentage of their applications run on containers.

AI- and ML-driven intelligence in data protection can take MSPs’ services to a new level. But this doesn’t require them to develop their own AI and ML training models. They can choose cloud data management platforms with pre-built AI and ML engines.
Minimizing customers’ risk profile
Given the complex nature of multicloud and hybrid cloud IT environments, there’s every chance that MSPs and their customers won’t find out if all crucial data is protected until it’s too late.

Redstor’s AI-powered technology proactively highlights gaps in protection:

- **Malware detection and removal**: AI isolates suspicious files for removal when backups are first performed, enabling organizations to perform a malware-free recovery later, while machine learning with fast community feedback on zero-day threats enables earlier identification of malware, providing an extra layer of protection.

- **Spotting trends**: MSPs can identify gaps in data protection, point out what may no longer need to be guarded, and create upsell opportunities.

- **Data tagging and categorization**: AI recognizes a data subject within a file and will then look for highly sensitive personal identifiers, categorizing a file depending upon its content. This allows organizations to not only understand where their most important data is being stored but also identify risk and re-allocate storage or permissions to reduce or remove that risk.

The next step
MSPs require purpose-built solutions — a simple, smart, cloud-native platform that protects data residing on infrastructure, in the cloud, and in containerized environments, as well as an array of SaaS applications such as Microsoft 365, Google Workspace, Salesforce, and Xero. With a single, intuitive, and multitenant app, MSPs can take immediate advantage of innovations with simple weekly or monthly updates, all on the same revision — and no longer forced to download multiple patches to a multitude of boxes.

About Redstor
Redstor offers MSPs best-in-class revenue retention, bigger margins, simple pricing, powerful marketing tools, and 24 x 7 support. Built for the cloud and fast to scale, the Redstor platform unifies the protection of modern, legacy, and SaaS infrastructure via a single app (RedApp). Breakthrough streaming technology delivers instant data access and mobility, bringing users back in seconds after outages, while unlocking all the benefits of a cloud-first model. AI polices backups to identify and isolate malware for safe restores. With just three clicks to get started, and no hardware or integration needed, Redstor is purpose-built for the MSP growth agenda.
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.