FROST & SULLIVAN

THE DATA PROTECTION GUIDE FOR ENTERPRISE MODERNIZATION

*Advanced, Complete Data Protection a Necessity
for Improving Competitive Positioning*
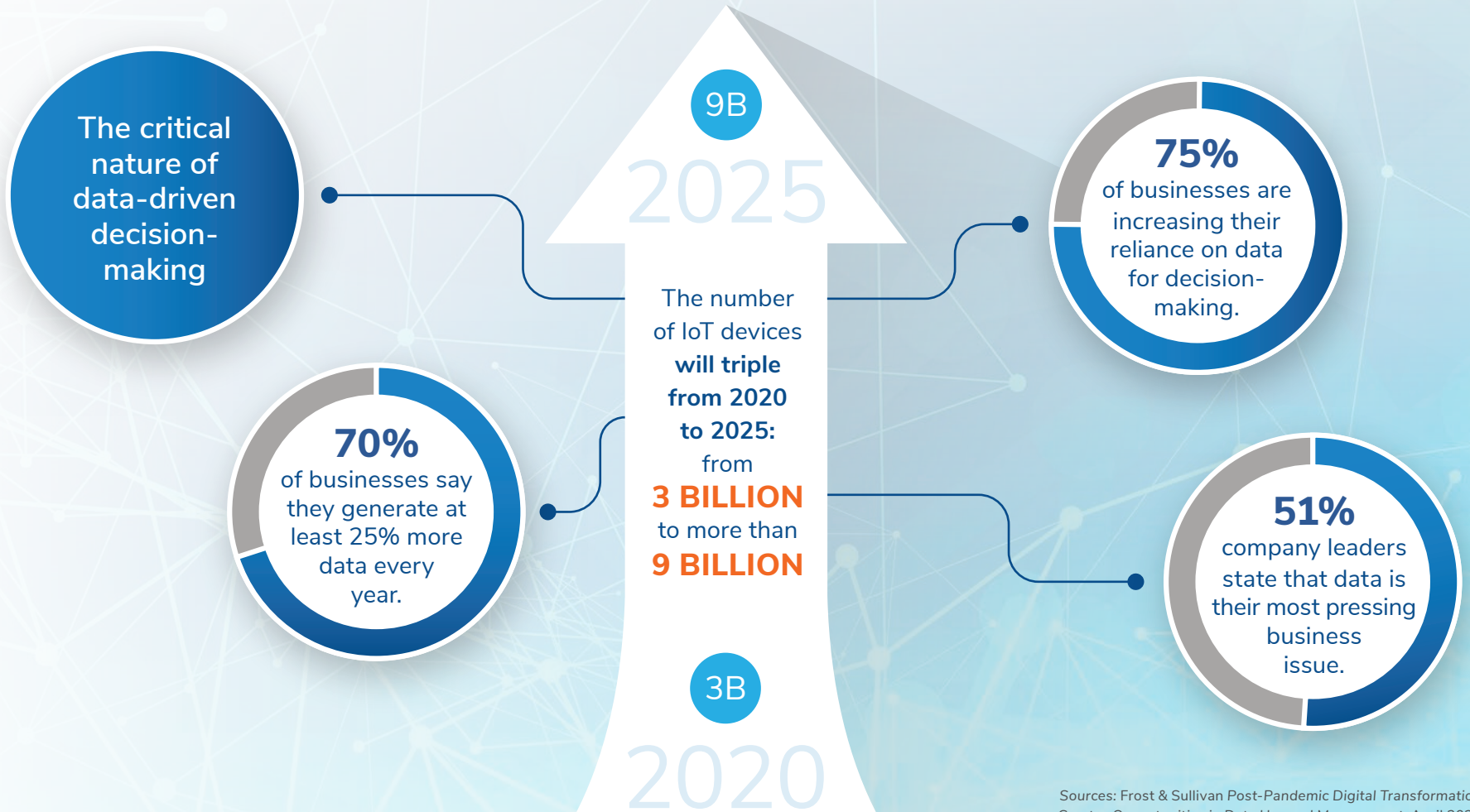
FROST & SULLIVAN VISUAL WHITEPAPER

frost.com

CONTENTS

FROST & SULLIVAN

Data Protection Challenges

Business data is growing across multiple facets of the modern enterprise, and new types of information generated by new sources are increasingly critical to operations. Backup reliability has decreased in recent years even as digital transformation activities accelerate.

GROWTH IN NEW SOURCES OF DATA

The critical nature of data-driven decision-making

9B

2025

The number of IoT devices **will triple from 2020 to 2025:** from **3 BILLION** to more than **9 BILLION**

3B

2020

75% of businesses are increasing their reliance on data for decision-making.

70% of businesses say they generate at least 25% more data every year.

51% company leaders state that data is their most pressing business issue.

F R O S T & S U L L I V A N

IT Priorities and Gaps

Business struggle with how to manage data

Cloud usage is growing at double digits, yet 67% of businesses struggle with cloud adoption, making them vulnerable as the onus of securing data on the cloud often falls on the client.

Challenges with in-house IT capabilities, modern data protection adoption, and legacy systems stymie modernization efforts.*

BACKUP RELIABILITY HAS DECREASED IN RECENT YEARS EVEN AS DIGITAL TRANSFORMATION ACTIVITIES ACCELERATE
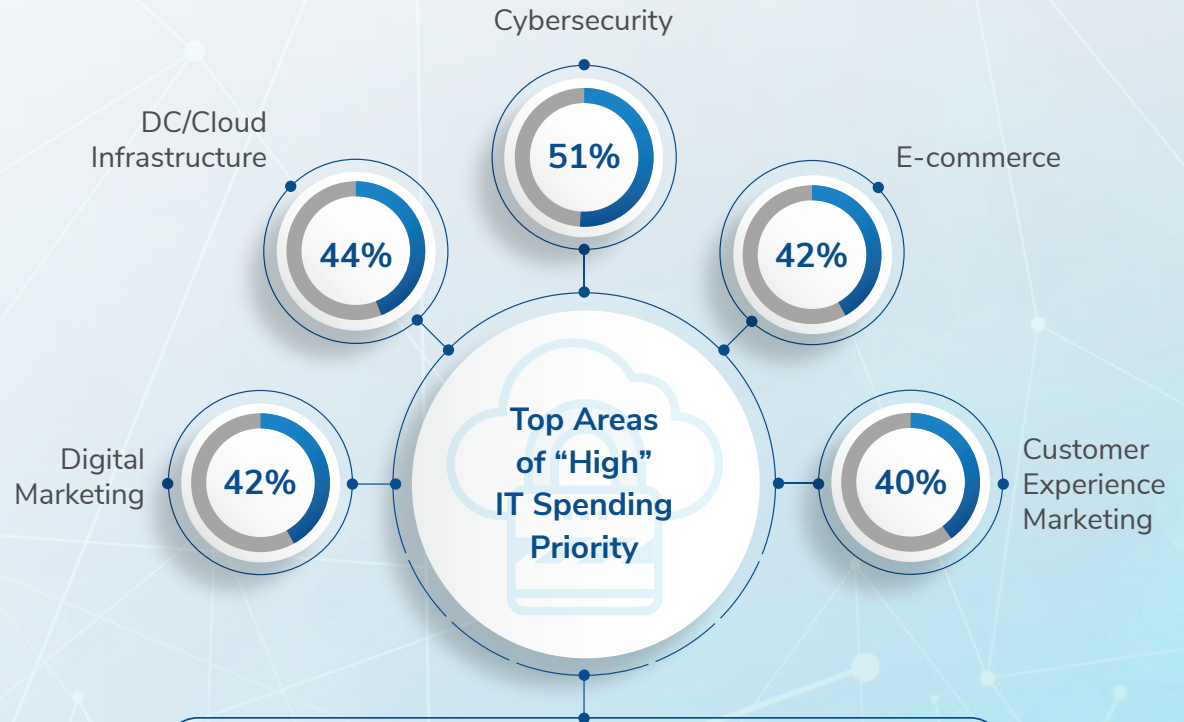
As many as **37% of backups** have errors or cannot be completed within the allotted time period.

Another **34% do not restore** within the service-level agreement.*

SECURITY IS A GROWING CHALLENGE

Cybersecurity
51%

DC/Cloud Infrastructure
44%

E-commerce
42%

Digital Marketing
42%

Top Areas of "High" IT Spending Priority

Customer Experience Marketing
40%

As cyber threats grow, security reigns as the top priority for IT teams, but data backup and recovery do not always keep step with other digital transformation investments.

Top three areas selected by 1,464 IT and business executives

FROST & SULLIVAN

Handling the Demand for Digital Customer Experience (CX)

Rapid cloud adoption rates are because of the demand for customer experiences that are digital, personal, and competitive. Public cloud revenue topped $76 billion in 2020 and will continue to grow at double digits through at least 2025. More than 85% of businesses use, or will use, cloud by 2022.
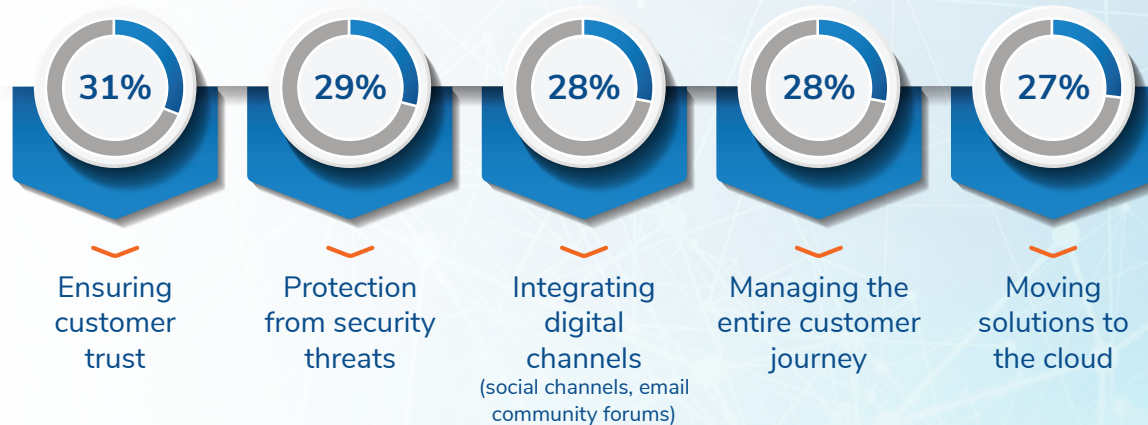
An estimated 80% of digital customer applications will be cloud-based by 2023. Customer experience is the #1 priority for IT budgets, followed by customer trust and security. Every customer interaction and data transaction across devices and infra-structures exposes a potential weak point that threatens positive customer interactions.

Server and network outages, application software outages, storage hardware failures, and cybersecurity events are the leading causes of data outages.* Any data storage outage or failure can kill customer loyalty. To retain brand integrity, organizations must prioritize data backup and recovery.

DEPARTMENT PRIORITY FOR DIGITAL TRANSFORMATION BUDGETS**

1 (tie) — Customer Care Product Management

2 — Marketing

3 — Sales

4 — Accounting & Finance

5 — Executive Management

6 — Manufacturing

7 (tie) — Human Resources R&D

Which departments are the top priorities for investments in digital transformation?   N=3262

TOP CX PRIORITIES, 2021 TO 2022**

31%	29%	28%	28%	27%
Ensuring customer trust	Protection from security threats	Integrating digital channels (social channels, email community forums)	Managing the entire customer journey	Moving solutions to the cloud

Top customer experience (CX) priorities for your company over the next two years.   N=1378

FROST & SULLIVAN

The Dramatic Shift to Remote Work

Fully or partially remote work scenarios have become the norm. The pivot to remote workforces combined with virtualized customer experiences accelerated digital transformation: 44% of organizations hastened technology purchases in 2020.

Vulnerabilities can arise from employees accessing systems from personal devices and under-secured networks, yet organizations neglect data backup and recovery upgrades when accelerating their digital transformation, undercutting security protection and forgoing data optimization opportunities.

WORK-FROM-HOME FLEXIBILITY IN SELECTED COUNTRIES

80%	69%	68%	60%	58%	51%	32%
GERMANY	US	UK	FRANCE	INDIA	SINGAPORE	JAPAN

REVERSAL IN ATTITUDES
TOWARD REMOTE WORK (GLOBAL, 2019-2020)
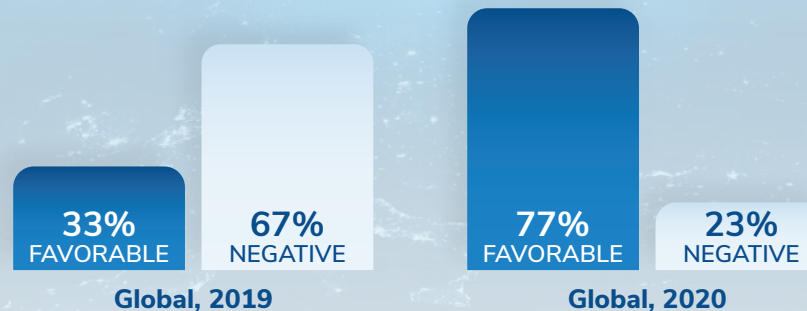
33% FAVORABLE	67% NEGATIVE	77% FAVORABLE	23% NEGATIVE
Global, 2019		**Global, 2020**	

FROST & SULLIVAN
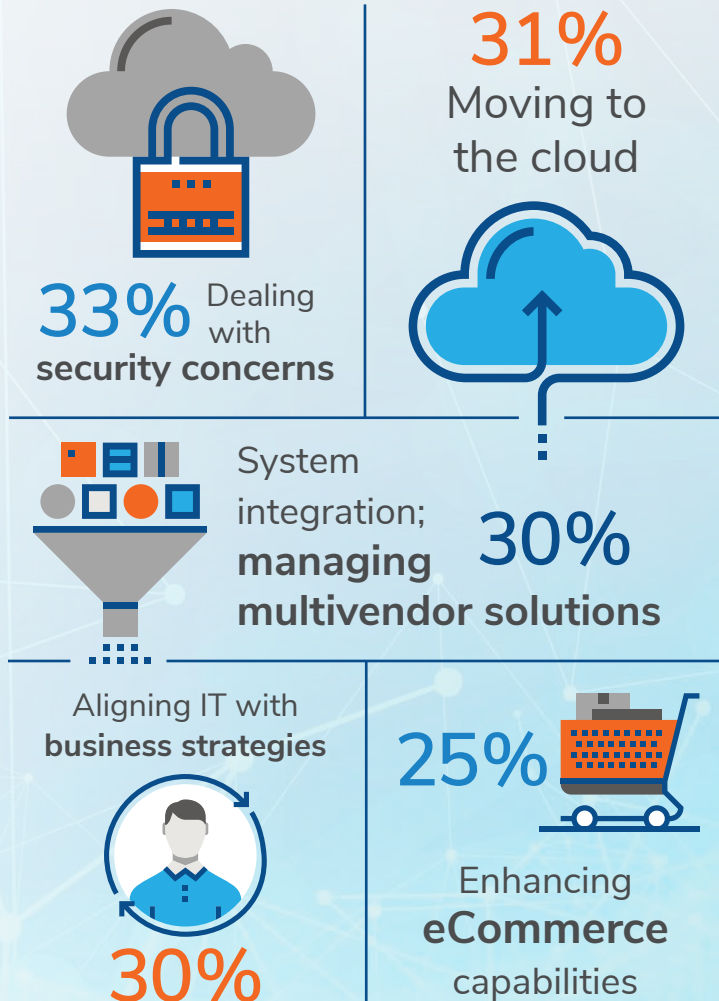
Fast-tracking of Data Protection

Security concerns: Booming ransomware, smarter phishing tactics, and the surging number of connected devices accessing data and systems from unsecured networks all challenge modern enterprises. A thorough security strategy with robust, agile, and flexible data backup and instant recovery is the last line of defense, but must work in the cloud, on premises, and at the edge.

Cloud migration: Advanced platforms secure data and deliver comprehensive, cloud-native backup and rapid recovery regardless of infrastructure, bridging gaps and ensuring RPO and RTO meet SLAs. However, the responsibility for backup and recovery falls on the customer rather than their cloud provider, which are not responsible for backing up and securing data hosted on their clouds. This leaves clients susceptible to gaps in the ability to recover their data when something goes wrong.

System integration and multiple vendors, and aligning IT and business strategies: Frost & Sullivan research shows that 43% of businesses use multicloud services. On average, organizations use three public cloud providers*. Engaging a single vendor with a comprehensive platform streamlines interactions and ensures that gaps are covered, especially in multicloud scenarios. IT teams can focus on business optimization instead of juggling vendor relationships. Cutting-edge data protection solutions also support rapid and secure data mining and forensic and root cause analysis without interrupting or slowing daily operations.

Improving eCommerce without sacrificing customer data security: Growth requires the flexibility to expand online commerce without being hindered by data security or backup challenges. Modern data backup and security ensure that PII remains private, accessible, and compliant with growing global requirements. Leading solutions also provide a sandbox for DevOps to test new apps in a real-world configuration but without the security risks.

TOP IT CHALLENGES

31% Moving to the cloud

33% Dealing with **security concerns**

System integration; **managing multivendor solutions** **30%**

Aligning IT with **business strategies** **30%**

25% Enhancing **eCommerce** capabilities

What will be the top 3 challenges your IT/Telecom department will face over the next two years?

FROST & SULLIVAN

Unique Challenges Facing Enterprises

Large enterprises in particular have unique circumstances not typically experienced by small and medium businesses that make security, efficiency, and compliance particularly difficult.

CYBERSECURITY TARGETS

- House and manage large volumes of valuable customer and business data

- Higher revenue and greater threat to reputation makes them more likely to be ransomware targets

- Employees, customers, and value chain partners mean more people accessing data and systems, creating more openings for threats

OPERATIONAL COMPLEXITY

- More workloads, apps, updates and changes from having multiple products and departments, and varying IT processes due to global expansion or M&A

- Global presence means higher likelihood of having on-prem and cloud data in more places, different IT departments, and varying compliance needs

- Greater use of hybrid- and multi-cloud environments

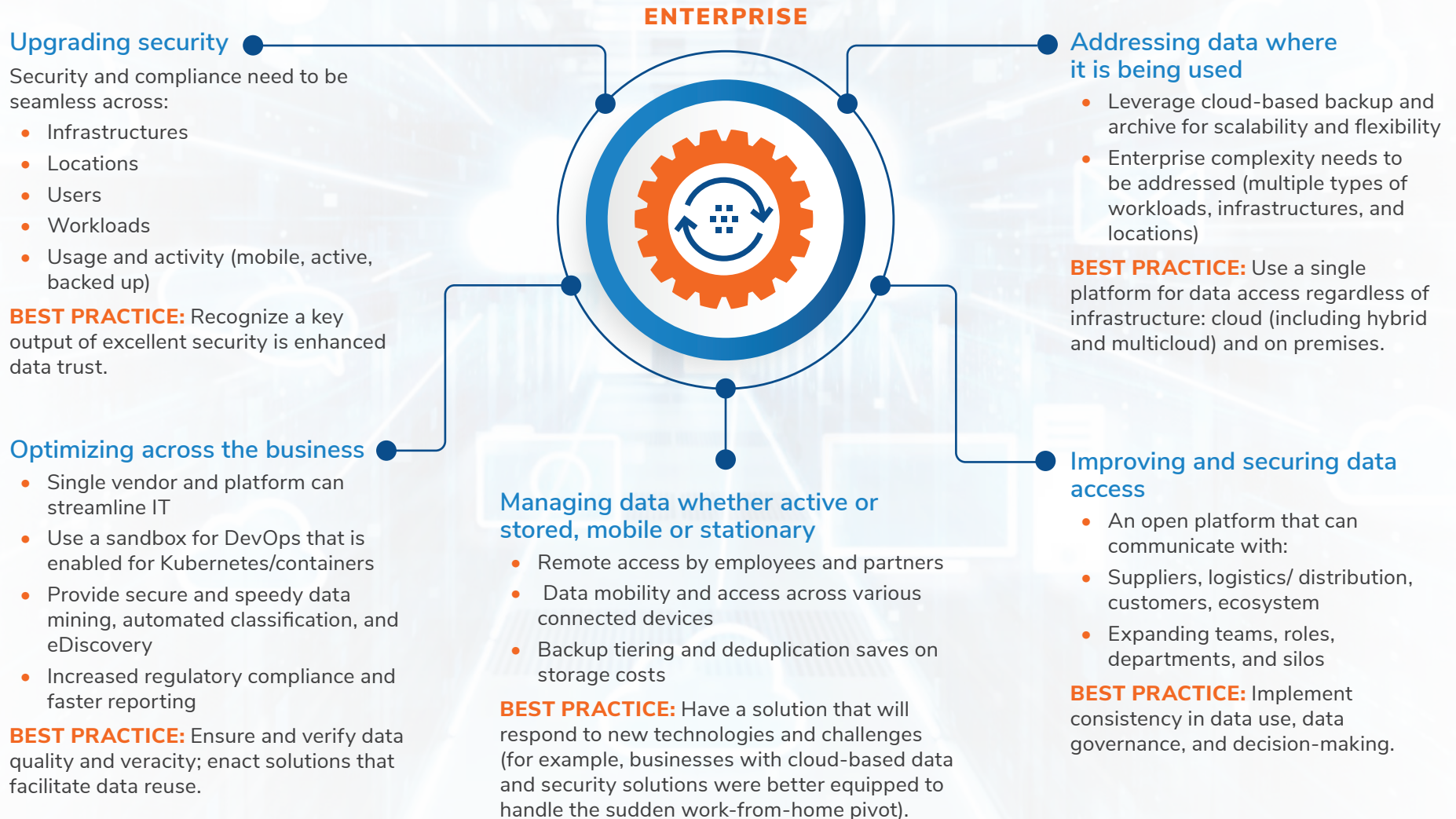- Organizational visibility more difficult— and more important—to attain across multiple locations and silos

REPUTATION

- Multiple stakeholders, investors, partners, customers, and broad economic impact make data breaches with large enterprises more visible and problematic than SMBs

- Market leaders in particular may be under intense regulatory compliance and scrutiny

FROST & SULLIVAN

Securing the Modern Enterprise Ecosystem

Organizations share data and system access with customers, vendors, and other ecosystem partners to optimize internal efficiencies and bring competitive solutions to market. Data backup and recovery should foster—not hinder—growth and innovation.

ENTERPRISE

Upgrading security

Security and compliance need to be seamless across:

- Infrastructures
- Locations
- Users
- Workloads
- Usage and activity (mobile, active, backed up)

BEST PRACTICE: Recognize a key output of excellent security is enhanced data trust.

Addressing data where it is being used

- Leverage cloud-based backup and archive for scalability and flexibility
- Enterprise complexity needs to be addressed (multiple types of workloads, infrastructures, and locations)

BEST PRACTICE: Use a single platform for data access regardless of infrastructure: cloud (including hybrid and multicloud) and on premises.

Optimizing across the business

- Single vendor and platform can streamline IT
- Use a sandbox for DevOps that is enabled for Kubernetes/containers
- Provide secure and speedy data mining, automated classification, and eDiscovery
- Increased regulatory compliance and faster reporting

BEST PRACTICE: Ensure and verify data quality and veracity; enact solutions that facilitate data reuse.

Managing data whether active or stored, mobile or stationary

- Remote access by employees and partners
- Data mobility and access across various connected devices
- Backup tiering and deduplication saves on storage costs

BEST PRACTICE: Have a solution that will respond to new technologies and challenges (for example, businesses with cloud-based data and security solutions were better equipped to handle the sudden work-from-home pivot).

Improving and securing data access

- An open platform that can communicate with:
- Suppliers, logistics/ distribution, customers, ecosystem
- Expanding teams, roles, departments, and silos

BEST PRACTICE: Implement consistency in data use, data governance, and decision-making.

FROST & SULLIVAN

Success Story: Airbus Defense and Space

Multibillion-dollar aerospace market leader Airbus's Defense and Space division plays a critical role in the satellite communication market. It monitors and tracks data across a satellite's 20-plus-year life cycle: from assembly through launch, orbit, and into deorbiting. The backup and recovery of satellite telemetry data are imperative in ensuring safety and operations for major global communication networks.

THE CHALLENGE

Airbus's Toulouse Satellite Operations Center (TSOC) manages satellite telemetry data and provides command and control services. Data integrity is closely tied to the business continuity of TSOC's clients, which include major telecom, mobile network, radio, and television companies. As such, TSOC cannot afford any interruptions in data availability, as this information feeds directly into critical project phases such as satellite positioning. As its business and data volume expanded, TSOC sought to upgrade backup, recovery, and protection to safeguard its ability to deliver industry-leading services.

THE PROCESS

TSOC quickly decided to move towards a proposal from Veeam®, which was convincing in terms of performance, technical feasibility and cost efficiency. The team was very interested in the integration between Veeam ONE and Veeam Backup & Replication™. Veeam's solutions provided TSOC the flexibility it needed to ensure operational continuity for existing command and control satellite projects and for years to come. Veeam was able to protect more than 550 virtual machines and 25TB of data, and provide the data availability needed for 24/7 satellite monitoring.

THE OUTCOME OF THE PARTNERSHIP RESULTED IN:

- Reducing the time it took to restore classic VMs from several days to 20 minutes

- Ensuring that backup, recovery, and availability of data will to grow and evolve with TSOC for at least the next 15 years

- TSOC can confidently expand on-premises and cloud-based data operations as needed, having Veeam's protection, backup, and recovery regardless of infrastructure

FROST & SULLIVAN

Success Story: SodaStream

SodaStream's multibillion-dollar global business is a leader in the sparkling water space. It needs fast, efficient, and secure operations to supply over 80,000 retailers across 45 countries.

THE CHALLENGE

SodaStream's ingenuity and innovation has led it to be the top sparkling water brand worldwide. Achieving this success as a manufacturer requires volumes of data feeding into numerous systems and processes, all which have to be flexible, secure, and agile. SodaStream realized it needed to upgrade its old data recovery system, which was a combination of multiple solution providers and tape-based backup. This complex matrix of processes was costing the company time, was a security risk, and carried the potential for data recovery failure.

THE PROCESS

SodaStream partnered with Veeam for its enterprise-ready backup and disaster preparedness solution, Veeam Availability Suite. The solution provides fast and consistent backup and recovery across on-premises and cloud infrastructure, as well as across divisions (manufacturing, business intel, finance), which is necessary to ensure that critical systems are recovered quickly.

THE OUTCOME OF THE PARTNERSHIP RESULTED IN:

- Cost savings including those equivalent to half of an FTE plus $25,000 per year that SodaStream had been paying in tape costs

- Ensured SOX compliance

- Monitoring and report across the IT so as to avert any issues that may impact manufacturing

- On-premises infrastructure can be backed up to the cloud, enhancing disaster recovery capabilities

- Simplification, standardization, and efficiency across IT in the organization

Sources: https://www.veeam.com/success-stories/sodastream.html
www.sodastream.com
Frost & Sullivan analysis

Next Steps for Modernizing your Data Protection

When it comes to migrating key workloads—like your ERP suite—to the cloud, what are the key factors a managed service provider should bring to the table?

Consider:

➤ **Identify challenges and hunt down potential gaps.**
How has the business addressed changing customer demand and workforce needs? Have cybersecurity threats expanded? (If they have not... are you sure?) Is dynamic and active data backup and recovery an integral, and recently updated, part of the security strategy, or has it waned behind other upgrades?

➤ **Consider both business and IT goals when prioritizing investments.**
Is IT focused on core functions or managing multiple vendors? How long does root cause or forensic analysis take? Are data security compliance and reporting activities automated, efficient, and transparent, or lengthy and opaque?

➤ **Move forward quickly to stay secure, competitive, and foster growth.**
An advanced data backup and recovery solution goes beyond ensuring that growing volumes of data are secured and available as needed. Modern solutions will also help businesses ensure the right level of storage and security for different types of information, reducing storage costs and enabling near-real-time recovery. They will also create a virtual environment populated by real and accurate backed-up data so that new apps work right upon launch and any data mining activities do not slow down the rest of the business. Using a provider that unifies data backup and recovery in a single, cloud-native platform frees the IT team for other core tasks and allows a business to focus on business growth and competition.

FROST & SULLIVAN

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion

FROST & SULLIVAN