IDC

A Framework to Earn and Sustain Customer Trust, Mitigate Risk, and Drive Revenue Growth

June 2023

Authors:
Sudhir Rajagopal
Research Director, Future of Customer Experience
Grace Trinidad
Research Director, Future of Trust

IDC #EUR150405923

An IDC InfoBrief, Sponsored by

orange Business

Future-proof business resilience and growth with a framework to earn and sustain customer trust

Enterprises must work harder for every dollar their customers spend. Their ability to both utilize and protect data to boost trustworthiness has become the primary market differentiator.

But future value exchange is premised on data insights that hold key to earning and sustaining customer trust.

Governments globally have created a complicated patchwork of data policies and regulations that organizations must navigate.

Enterprises can build a foundation of trust from the infrastructure layer up to the customer engagement layer. Working alongside a trusted partner can help enterprises operationalize and scale customer-centric trust outcomes.

Investment in a foundation of trust pays dividends — IDC research finds that investment in security, privacy, compliance, and environmental and social governance (ESG) results in improved business outcomes and higher ROI.

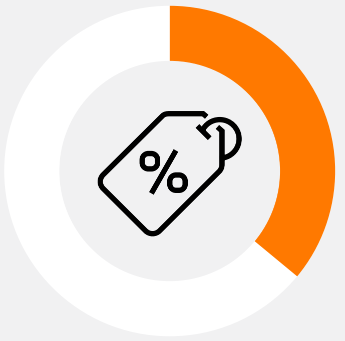
Trusted partners differentiate themselves and lead their industry peers in their ability to provide an enhanced delivery experience, and with their solution capabilities in security, compliance, and ESG.

Enterprises must work harder for every dollar their customers spend; their ability to utilize and protect data to boost trustworthiness is the primary market differentiator

1

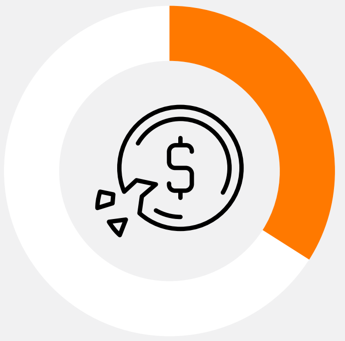
Acceleration of interconnected economic uncertainty. Business strategies are being impacted by risks stemming from inflation, recession, labor market shifts, and geopolitical turmoil, which have diminished consumer spending power and intensified competition. Percentage of enterprise leaders who are most concerned about the following risks that will impact their technology strategy[1]:

36%



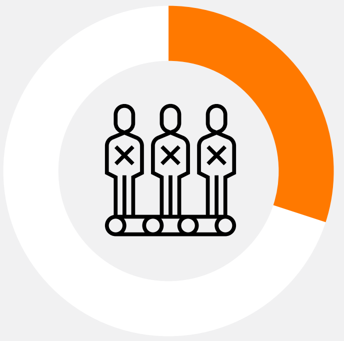
Inflation pricing that exceeds budget expectations

34%



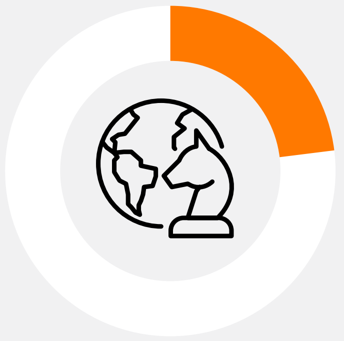
Recession impact on business revenue

30%



Staffing/labor shortages

23%



Geopolitical turmoil altering tech strategies

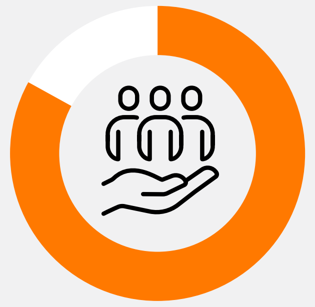
Value exchange between customers and businesses will be anchored in data

2

- Digital-first organizations see insights from customer and operational data as the primary fuel to unlock new business value as it enables them to drive loyalty through service excellence and cross- and up-sell a wider range of products and services.
- IDC's Global Datasphere forecast estimates that the volume of data in the world is expected to double by 2026 (currently at over 100,000EB). Data insights hold the key to anticipating customers' needs, preempting customer problems, and becoming more resilient in the face of disruption.

Customers trust firms that understand their needs but protect their privacy

3



83%[2] of customers say that how companies treat and protect data impacts their trust and confidence in a company. Mitigating risks that threaten digital trust is enterprises' number 1 challenge. Striking the balance between data utility (ensuring data is accessible, complete, and timely) and data privacy (including protecting data flows across hybrid cloud, edge, and on-premises infrastructure) is key.

- Digital sovereignty has become an imperative for organizations and is quickly becoming the centerpiece of trust efforts, as enforcement of GDPR and regional and vertical industry laws and regulations increases.
- Privacy is one of the pillars of trust, and high trust is a prerequisite for customer willingness to share the personal data required to generate high-quality and meaningful AI/ML insights.
- Limiting data collection to only that which is necessary for business brings environmental impact and cost advantages, decreasing the need for data storage.

Evolving threat environment has a direct impact on the bottom line — data breaches and privacy violations erode trust

4

- IDC's *CEO Sentiment Survey* shows that 30% of CEOs see new data sharing and compliance risks as having the greatest impact on their business by 2024. External research estimates that the average cost of a data breach could increase to $4 million by 2024.
- Investment in trust programs (including security, privacy, compliance, and ESG technologies) brings improvements in key business outcomes.

[1] IDC Future Enterprise Resilience and Spending Survey, January 2023
[2] IDC 2022 B2B Technology Buyer Survey

Future value exchange is premised on data which holds the key to earning and sustaining customer trust

Customer trust is the currency for future business resilience and growth

Trust is the result of a virtuous cycle of excellent customer experiences with a brand. Trusted brands get bought, used, and recommended more; eventually end up with a higher proportion of loyal customers; and are more profitable. IDC research shows that companies' actions regarding security, privacy (including how customer data is used and protected), and environmental and social governance efforts significantly impact customer trust.

Engendering customer trust:

Balance the dichotomy: data insights versus privacy

79% of customers expect businesses to offer insights-based contextualized engagement.

But

59% have privacy concerns about enterprises knowing their information.

Sustain data integrity for customers

Trust in a company's use of customer data is **as important as** product features or performance, in influencing customers' engagement and purchase decisions.

83% of customers say that how companies protect their data impacts their trust in the company.

Prepare for tightening privacy and security regulations

More than half

(55%) of enterprises report that regulatory compliance (e.g., GDPR) is the main factor in deciding how and where they store enterprise data.

48% of enterprises say data sovereignty factors highly in future technology architecture decisions.

Source: IDC Global Future of Manufacturing Survey, November 2022, n = 160

Governments globally have created a patchwork of data policies and regulations that organizations must manage

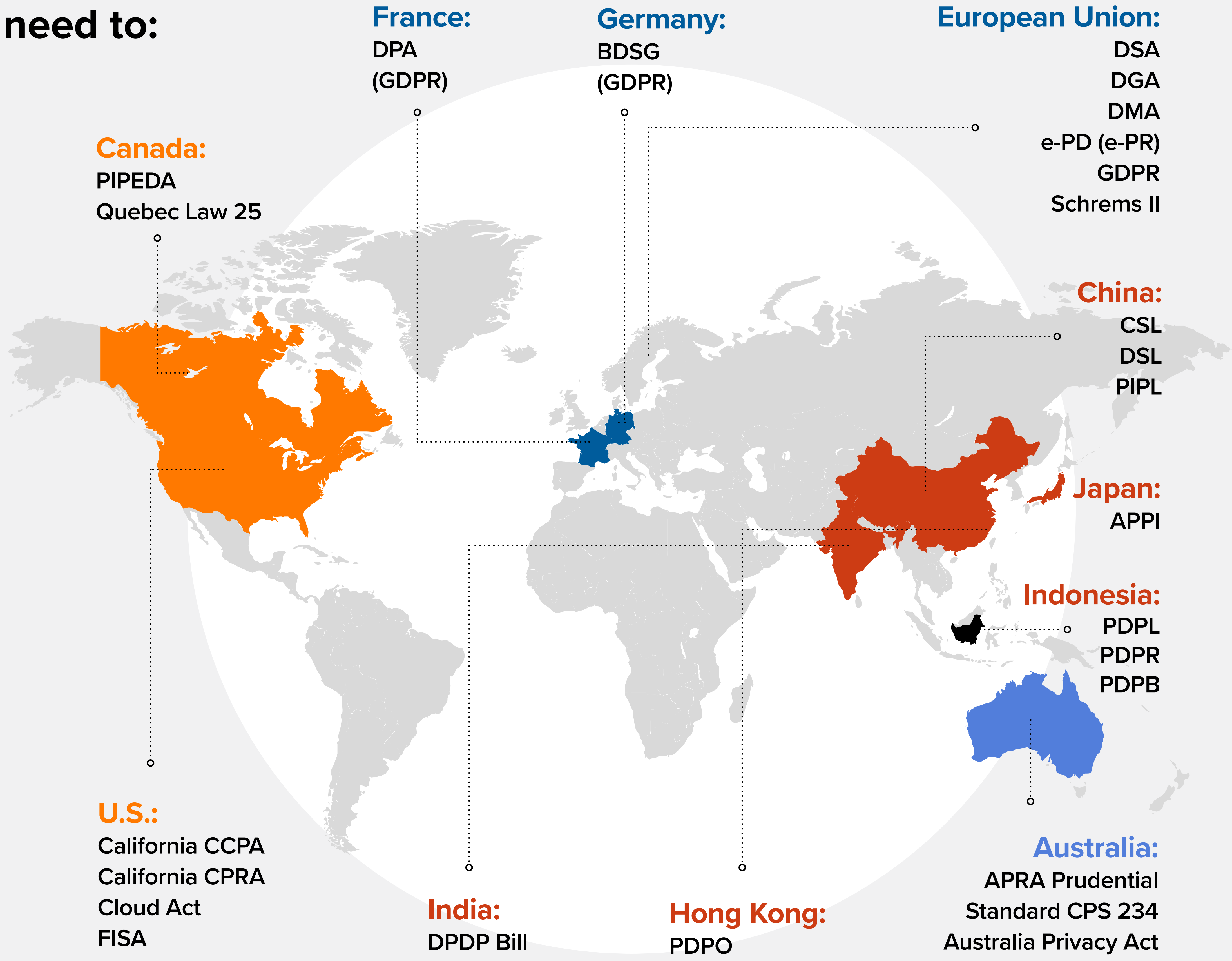
Organizations must navigate an increasingly complicated landscape, and need to:

Ensure more robust and resilient information security infrastructure

Protect the privacy of data subjects

Provide individual consent and control over use of personal data — collect, use, and disclose personal data use for legitimate purposes and retain this data only as long as necessary

- Schrems II verifies the data protection laws of recipient countries — companies must ensure that data protection is equivalent to the EU and document their assessment of all risks. Key tasks include:
  - Updating standard contractual clauses (SCCs) for international data transfers
  - Updating mapping of cross-border data processing — maintaining descriptions of operations, destinations, recipients, transfer tools, types of personal data, and categories of data subjects
  - Avoiding data processing activities that involve personal data transfer to the U.S.
- The Cloud Act creates a new statutory basis for deference to the laws of a foreign jurisdiction. The Foreign Intelligence Surveillance Act (FISA) continues to allow for surveillance of U.S. surveillance targets if they are outside the United States.
- The China Data Security Law (DSL) and Personal Information Protection Law (PIPL) stipulate that "core" and "important" data stored in China can't be provided abroad, regardless of where the data was initially collected. Data provenance is closely monitored and data verification and data transaction records must be retained. Consent from data subjects must be secured to transfer personal information to third parties.
- There are also many data governance and privacy standards that are specific to vertical industries and sectors. PCI DSS, for example, is the global standard to which any entity that transmits, stores, handles, or accepts credit card data must adhere.


France:
DPA
(GDPR)

Germany:
BDSG
(GDPR)

European Union:
DSA
DGA
DMA
e-PD (e-PR)
GDPR
Schrems II

Canada:
PIPEDA
Quebec Law 25

China:
CSL
DSL
PIPL

Japan:
APPI

Indonesia:
PDPL
PDPR
PDPB

U.S.:
California CCPA
California CPRA
Cloud Act
FISA

India:
DPDP Bill

Hong Kong:
PDPO

Australia:
APRA Prudential
Standard CPS 234
Australia Privacy Act

A winning combination of foundational trust solutions and a trusted delivery partner can help gain control over known and unknown future risks

Enterprises need to orchestrate trusted solutions, beginning from the infrastructure layer and working up to the customer engagement layer. A trusted delivery partner can operationalize the wide range of solutions and cultural changes that are needed to achieve trust-centric business outcomes at scale.

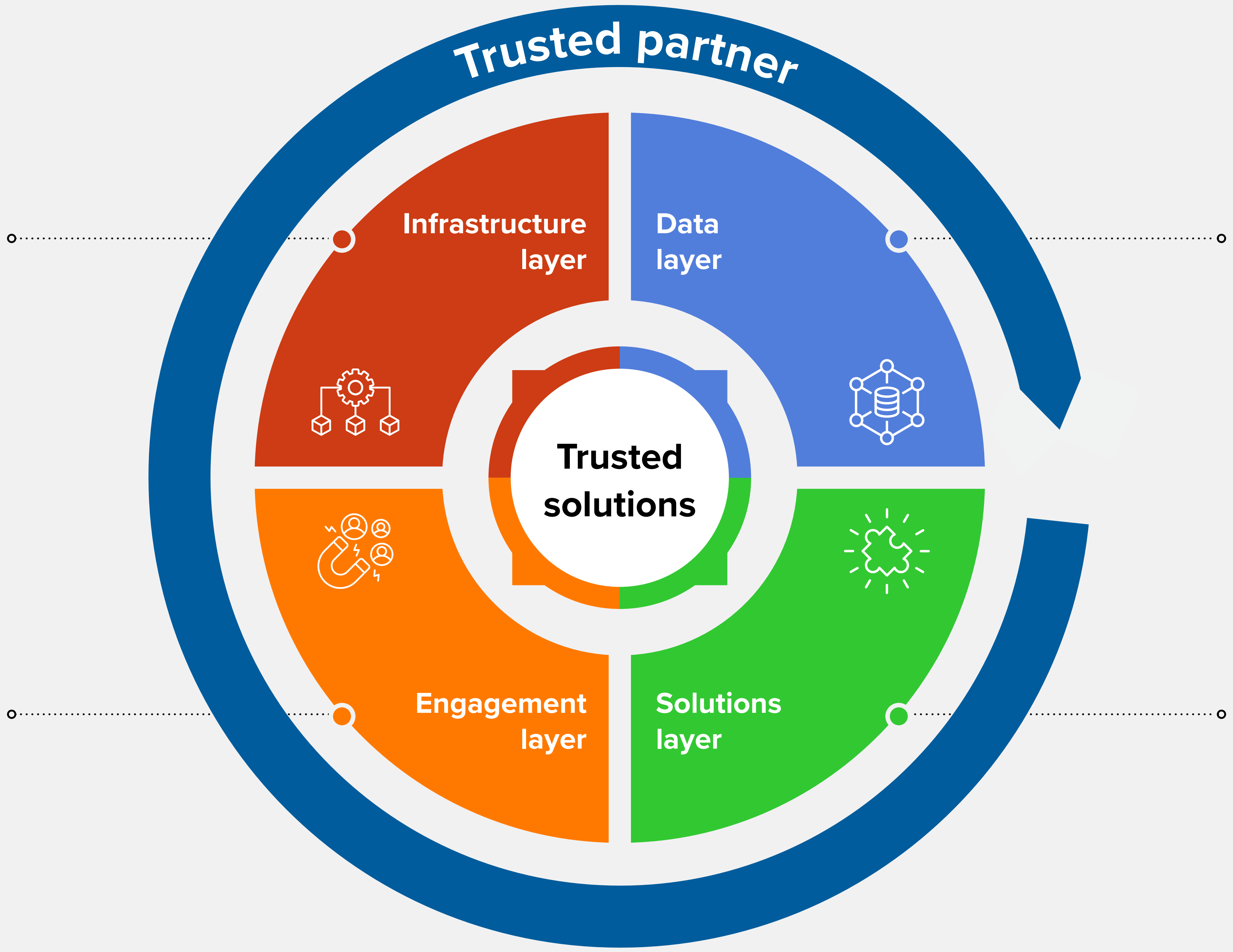
Secured infrastructure:

- Match security capabilities to the sensitivity of information assets
- Ensure your business continuity procedure takes into account the cost of downtime for each application
- Ensure your business continuity procedure takes into account the cost of downtime for each application
- Consider peer-to-peer encryption as part of your hybrid cloud networking solution
- Gain visibility of security data from endpoints, network traffic, and logs for faster threat detection and response
- Use zero-trust security to grant access to resources based on identity and context

Customer engagement:

- Notify customers that data is being collected, for what purposes, and how long it will be held
- Customers require notification about how data is retained and for how long
- Provide data usage consent options
- Use data tokens to enable customers to anonymously share data
- Develop trust and data breach messaging

Four foundational building blocks for trust solutions



Data life-cycle management:

- Collect data for specific purposes only
- Overcome the challenge of shadow data with a distributed data mesh architecture
- Ensure you can share data internally and across business ecosystems
- Avoid data bloat and reduce costs and your carbon footprint with data deletion
- Accelerate data analysis using AI/ML
- Employ edge computing for increased response and insight speed

Data privacy solutions:

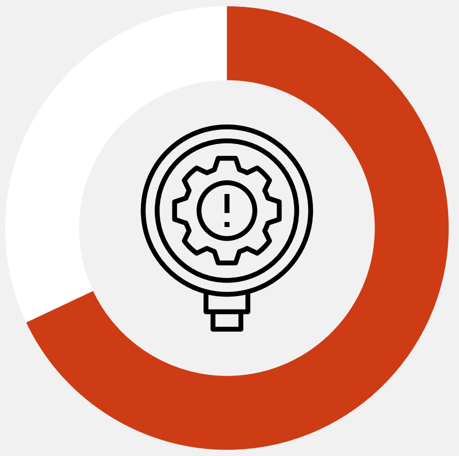
- Use data catalogs and integration tools to improve data discovery
- Map relationships between data entities and reduce redundancies
- Assess data risks (including third-party vendors) and automate data subject requests (DSRs)
- Update your standard data protection contractual clauses (SCCs) with geospecific information

Source: IDC Global Future of Manufacturing Survey, November 2022, n = 160

Infrastructure: Trust is built on secure and resilient infrastructure

Trusted partner
Infrastructure layer
Data layer
Trusted solutions
Engagement layer
Solutions layer

Trust is built on solid secured infrastructure. Without a strong foundation of security, the other antecedents to trust (privacy, compliance, and environmental and social governance) are not possible. Protecting employee, customer, and partner data is vital to be a good corporate citizen. The EU Data Governance Act (DGA) mandates a secure environment for the storage and processing of data.



IDC research finds that

68% of respondents identify **security as the top risk to digital trust.**[1] The key security features worldwide include backup and disaster recovery, encryption and key management, and threat detection and response.[2] Trusted businesses with strong security postures see greater operational resilience as a result of their investments.

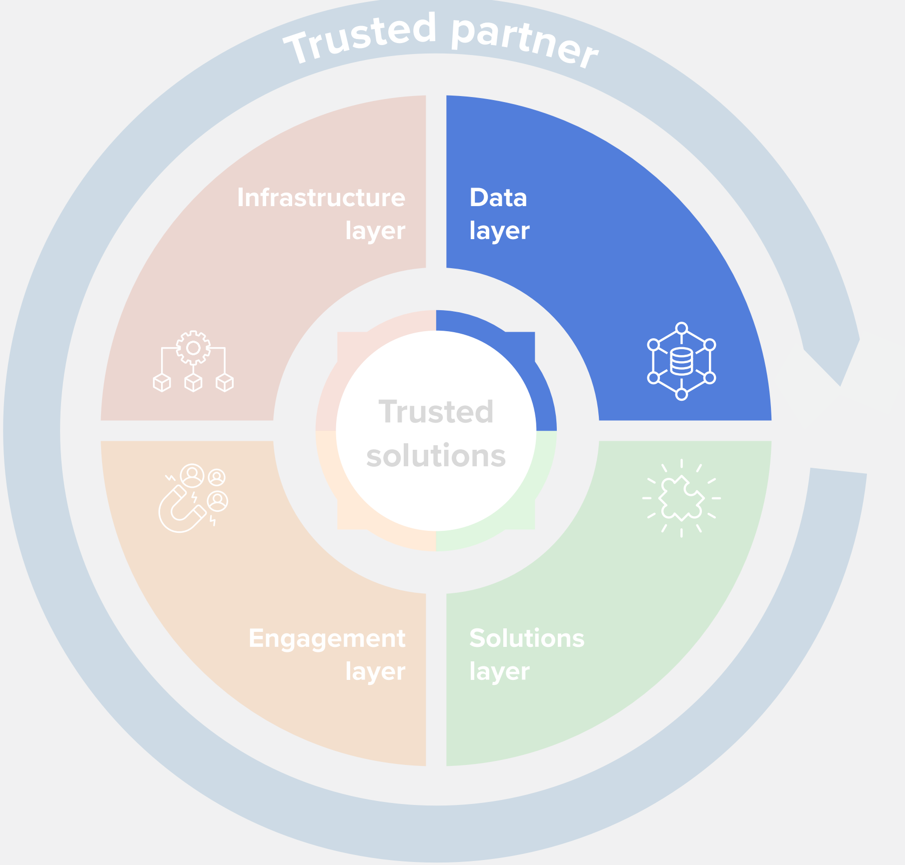
Areas of security ranked by importance

	Worldwide	EMEA	France	U.K.
1	Backup and disaster recovery	Backup and disaster recovery	Threat detection and response (endpoint, network, etc.)	Encryption and key management
2	Encryption and key management	Hardware and/or software supply chain vulnerabilities	Hardware and/or software supply chain vulnerabilities	Hardware and/or software supply chain vulnerabilities
3	Threat detection and response (endpoint, network, etc.)	Encryption and key management	Encryption and key management	Backup and disaster recovery

IDC research has found that worldwide respondents prioritize backup and disaster recovery, followed by encryption and key management. EMEA respondents, however, placed management of hardware and/or software supply chain vulnerabilities as the second most important area of security when evaluating cloud vendors.

[1] IDC Future Enterprise Resilience and Spending Survey, July 2021
[2] IDC Future of Trust Survey, January 2022

Data: Trusted partners manage the privacy and security of data through its life cycle: data collection, storage, use, sharing, archive, and destruction



Under GDPR, data subjects now have the right to know what data has been collected about them and how that data is processed. They retain the right to transfer personal data, the right to make changes to inaccurate data, the right to withdraw consent, and request the deletion of personal data. Data cannot be processed without first securing consent. Schrems II invalidated the Privacy Shield (the Safe Harbor mechanism), accelerating the adoption of data mapping and transfer reporting tools.

IDC research finds that

67% of respondents agree that digital sovereignty improves their ability to shape digital transformation efforts **in addition to enhancing customer and stakeholder trust in the organization.**

Data life cycle

Data creation/ collection	The point at which data is created or imported into the system. Data is also ideally classified at this stage, after which the appropriate security level can be applied.
Data storage	Storage is where security controls are employed to protect data, setting access controls, encryption, and data auditing.
Data use	Data in use is vulnerable to leakage or at risk of being compromised. Lack of coordination or misconfiguration of access or authentication between various services can compromise data. There is a significant issue with shadow data, which can be addressed with solutions such as data mesh.
Data sharing	Data leaves the system and is no longer under the purview/control of the originating system. Data loss prevention (DLP) and information rights management (IRM) can be used to detect anomalies when sharing and prevent unauthorized modification of data.
Data archive	Long-term retention based on organizational policies and regulatory requirements must ensure archived data can be successfully retrieved and read.
Data destruction	Permanent destruction of data based on user request or sensitivity classification.

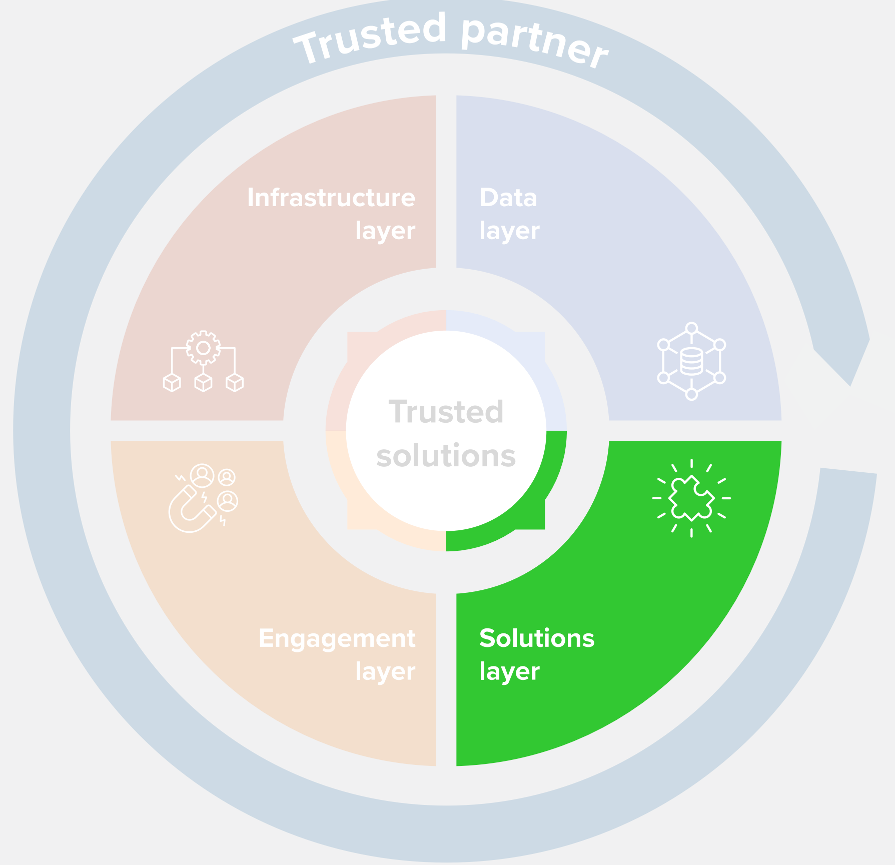
The top areas to manage digital sovereignty are investments in improved:

- Privacy measures and implementation
- Integrated risk management processes to include geographic parameters
- Organizational and regulatory compliance[1]

As we quickly move into a world mediated by data and determined by AI, organizations should remain aware of how and from whom their data is collected. **The data on which organizations base decisions needs to be complete and representative to mitigate the risk of AI/ML bias.** High trust is a prerequisite for customer willingness to share the personal information that brings high-quality organizational insight.

[1] IDC, Future Enterprise Resilience and Spending (FERS) Survey, May 2022

Solutions: Privacy solutions and emerging technologies exist to support trusted partners in GDPR and Schrems II compliance



A suite of services is emerging to meet the data management requirements of GDPR and Schrems II. These services specialize in data transfer risk assessments, vendor risk assessments, mapping data flow, consent monitoring and tracking, cookie compliance, data subject requests (DSR), data subject access requests, data rectification requests, and data erasure requests.

Areas of privacy ranked by importance

	Worldwide	EMEA	France	U.K.
1	DLP/IRM	Retention, erasure, and disclosure according to privacy regulations	Data obfuscation/confidentiality and data integrity (includes masking, randomization, encryption)	Standards and contractual safeguards
2	Data usage permissions and control	DLP/IRM	Retention, erasure, and disclosure according to privacy regulations	Retention, erasure, and disclosure according to privacy regulations
3	Data discovery, classification, and categorization	Data discovery, classification, and categorization	Monitoring, reporting, and transparency of privacy policies	Data usage permissions and control

The prevalence of hybrid work environments is accelerating the adoption of **zero-trust** frameworks to reduce the vulnerability of assets that employees must access.

Core tenets of zero trust: verification, least privileged access, and end-to-end encryption

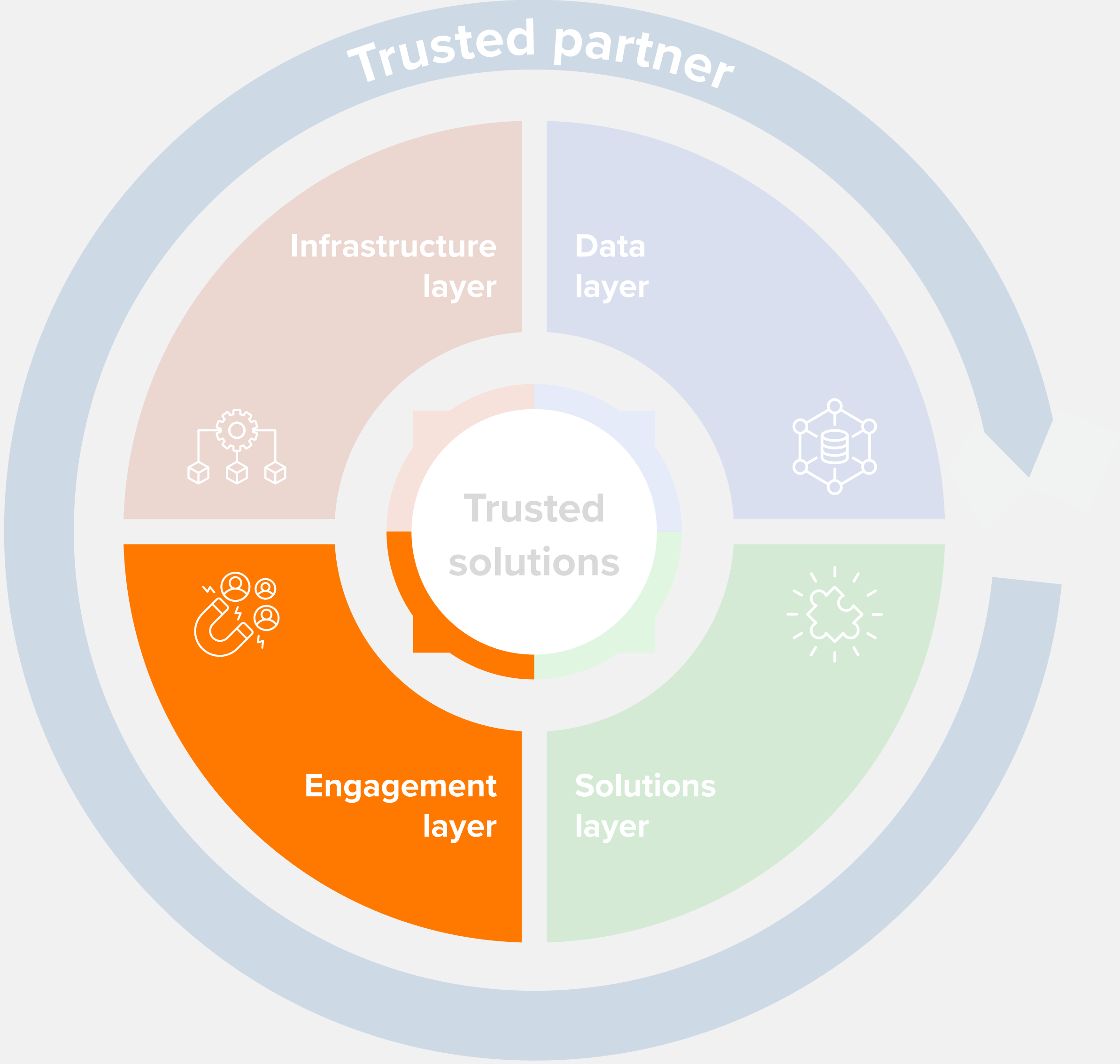
Organizational considerations when implementing zero trust: attack surface management, data security, and identity access management

Data protection and privacy tools to address regulatory requirements

Issue	Technology
Data discovery	Asset and data discovery
Data mapping	Data lineage and data privacy automation
Data identification	Data intelligence
Data risk reporting	Data mapping and vendor assessments
Consent management	Data consent automation
Data subject access requests	DSR automation
Protecting data in use	Zero-trust security (including confidential computing and decentralized identities)

Source: IDC Global Future of Manufacturing Survey, November 2022, n = 160

Engagement: Enterprises need to become ethical stewards of customer data, privacy, security, and the environment to sustain trust



As enterprises continue to innovate with new digital-first products and services, anticipating customers' needs and preempting problems and being resilient is crucial to sustain trust. At the same time customer data is no longer a commercial entitlement. Customers are willing to share their data in return for better overall products and services. Enterprises need to make the customer feel safe and secure in their management of that data and adhere to regulatory compliance practices.

IDC research finds that **40%** of enterprises globally are prioritizing customer trust and privacy initiatives, with **15.3%** reporting it as their number 1 priority.

Engage with permissible outcomes

- **60%** of enterprises are addressing regulations for collecting, using, and storing customer data as a top priority.
- In addition, enterprises will need to centralize customer privacy and consent policies and establish cross-enterprise tracking of customer consent and data subject access.
- Enterprises should also introduce metadata schema to represent and measure the proportions of zero, first, second, and third-party data, in addition to parameters that govern use such as timing, expiry, priority, and consent.

Embed customer data transparency

- Leading enterprises embed transparency regarding their use of customer data within their engagement processes and provide consent options to customers. As a result, these organizations see **higher levels of mutual trust** with their customer base.

Combat bias

- **Over two-fifths** of companies are addressing regulations for fair and ethical use of AI.
- IDC predicts that by 2025, 40% of the G2000 will promote ethical use of AI and data in marketing with other ESG initiatives, aligned to customer trust. This is forecast to boost their market share by 5%.

Research shows that investment in trust results in improved business outcomes and ROI

Why do we examine trust? Trust has been described as a “confident relationship with the unknown.” We can’t know everything in our complex and rapidly evolving world, but being seen as a trusted partner helps to mitigate business losses should adverse events occur. High trust creates a competitive edge and engenders customer loyalty, and building trust is a prerequisite to overcome consumer reluctance to share personal data.

In a 2022 worldwide survey conducted by IDC, **78%** of respondents said **investments in trust programs are a priority or a high priority for 2023. 80% of EMEA respondents indicate** the same.

IDC research finds that prioritized investments in trust programs, or investments in security, privacy, and compliance, are significantly associated with improved business resilience, operational efficiency, and sustainability worldwide.[1]

By using regression analysis, we can statistically examine the relationship between two or more variables of interest.

We answer the questions: Which factors matter most? Which can we ignore? How do those factors interact with one another?

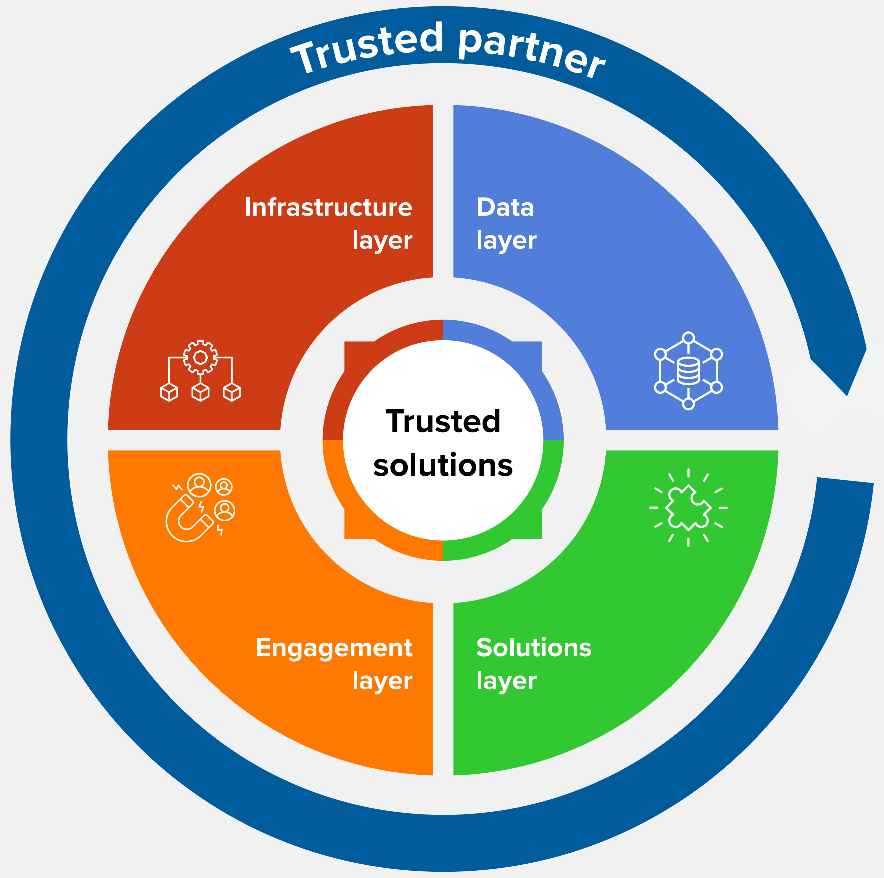
Business outcomes that are improved* as a result of investment in trust programs

Business resilience	Worldwide, investments in trust programs improve business resilience (worldwide, $R^2 = 0.03$). Companies that invest in trust set up the necessary security and privacy infrastructures foundational to establishing trust and recover more quickly during cyberattacks.
Operational efficiency	Worldwide (especially in Asia/Pacific) investment in trust programs improves operational efficiency (worldwide, $R^2 = 0.02$; AP, $R^2 = 0.06$), reduces the volume of data collected, and drives more organized approaches to data usage and privacy.
Sustainability	Worldwide ($R^2 = 0.02$), investment in trust programs boosts sustainability. ESG efforts are a pillar of trust and are increasingly important in buying decisions.
Profit	Asia/Pacific respondents see increased profit ($R^2 = 0.26$, $p < 0.001$) when they prioritize investments in trust programs.
Employee productivity	EMEA respondents see increased employee productivity ($R^2 = 0.05$) as a result of their investments in trust programs.
Business agility	Respondents from North America (U.S. and Canada) see increased business agility ($R^2 = 0.18$) as a result of their investments in trust programs.

[1] IDC, Future Enterprise Resilience and Spending Survey, Wave 5, June 2022

*Significance level set to $p < 0.05$

Suppliers that dominate the marketplace with efforts that enhance delivery experience, security, compliance, and ESG are seen as trusted partners



The IDC Trust Perception Index measures vendor performance, asking enterprises to rank what matters most to them and how key players perform. Beyond privacy and data management, trusted partners differentiate themselves from their peers based on their efforts in security, privacy, compliance, ESG, and experiential factors. It is both the capabilities and the culture of a provider that makes the difference in the service experience to drive long-term partnerships.

Core	**Security and compliance**	Security and compliance are critical, but they are table stakes. The top vendors perform to a similar standard when it comes to protecting data in line with all applicable data privacy and governance regulations, according to the IDC Trust Perception Index. Vendors that are trust leaders excelled in backup and disaster recovery; the availability of a skilled cybersecurity staff and leadership; identity, credential, and access management; and encryption and key management. Top performers also differentiated themselves on compliance by providing compliance certifications with global, national, and industry standards.
Differentiators	**Privacy and ESG**	Vendors that outperformed their peers in privacy and ESG efforts became the trust leaders in their markets, according to the IDC Trust Perception Index. Privacy leaders differentiated themselves on DLP and IRM and/or data obfuscation and data integrity, while ESG leaders differentiated themselves by having affordable pricing for sustainable offerings and services and/or the provision of KPIs on environmental sustainability and social impact.
	Experiential factors	IDC research finds that in a tightening economic environment, enterprises seek a trusted partner that can offer more than just solutions. They need support in reducing the complexity and costs of creating and managing trust infrastructure, with the right mix of consulting, integration, and support services, at the right price, backed by verticalized offerings, all under one roof.

International SOS chooses Orange to secure and manage critical applications in the AWS cloud in Europe

INTERNATIONAL SOS

International SOS, a global pioneer and leader in international health and security risk management, decided to move business applications to the cloud. This would improve efficiency, deliver releases faster to customers, and enable it to develop and launch new digital services. It also needed to address data sovereignty concerns for its customers regarding European compliance and the cancellation of the EU-UK Privacy Shield.

International SOS provides tailor-made health and security services for global organizations' mobile workforces 24 x 7. With its 27 assistance centers, reachable in 100 different languages, its 5,800 health professionals and its access to over 3,200 security specialists, International SOS helps companies to reduce exposure to and mitigate health, well-being, and security risks. Operating out of 90 countries, it looks after 82% of the Fortune Global 100 and 67% of the Fortune 500, and deals with over 3 million assistance calls annually.

Securing business-critical data in Europe

International SOS opted to go with Amazon Web Services (AWS) cloud to support its business development ambitions. The firm chose Orange as its trusted managed service provider, supporting business-critical applications in Europe. International SOS' European clients' confidential data is hosted by Orange in France, under the jurisdiction of EU laws regarding data storage and protection. In addition, Orange provides managed services, including a data encryption solution (AWS CloudHSM, a cryptographic service to create and maintain hardware security modules) to run European workloads on the AWS cloud infrastructure.

Providing a faster, enhanced service

Orange expertise as an AWS partner has enabled International SOS to optimize its European workloads on the AWS cloud to deliver faster, enhanced services to its customers. The AWS cloud solution brings richness in terms of capabilities and automation. On top of this, International SOS is also benefiting from an additional level of security from Orange Business. Orange strictly complies with EU regulations on data privacy and obeys EU rules regarding EU data stored in EU territories. The project highlights the trust and innovative partnership that has been achieved between Orange and International SOS.

27 assistance centers

Operates from 90 countries

5,800 health professionals

3 million assistance calls annually

Message from the Sponsor

Orange Business is a leading network and digital integrator which enables enterprises to have a positive impact on the world by helping them to accelerate digital business success.

The combined strength of its next-generation connectivity, cloud, and cybersecurity expertise, platforms, and partners provides the trusted digital foundations that enterprises need around the world to drive sustainable growth.

With 30,000 employees across 65 countries, Orange Business enables enterprises to accelerate digital transformation by orchestrating end-to-end secured infrastructure and focusing on delivering exceptional employee, customer, and operational experiences. More than 3,000 multinational enterprises, as well as 2 million professionals, companies, and local communities in France, put their trust in Orange Business, which is part of the Orange Group.

Orange is one of the world's leading telecommunications operators, with sales of €43.5 billion in 2022 and 287 million customers worldwide as of December 31, 2022. In February 2023, the group presented its strategic plan, "Lead the Future," built on a new business model and guided by responsibility and efficiency. "Lead the Future" capitalizes on network excellence to reinforce Orange's leadership in service quality.

For more information: www.orange-business.com

orange™ Business

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.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Corporate Headquarters
140 Kendrick Street,
Building B, Needham,
MA 02494 USA
508.872.8200
www.idc.com

Copyright Notice