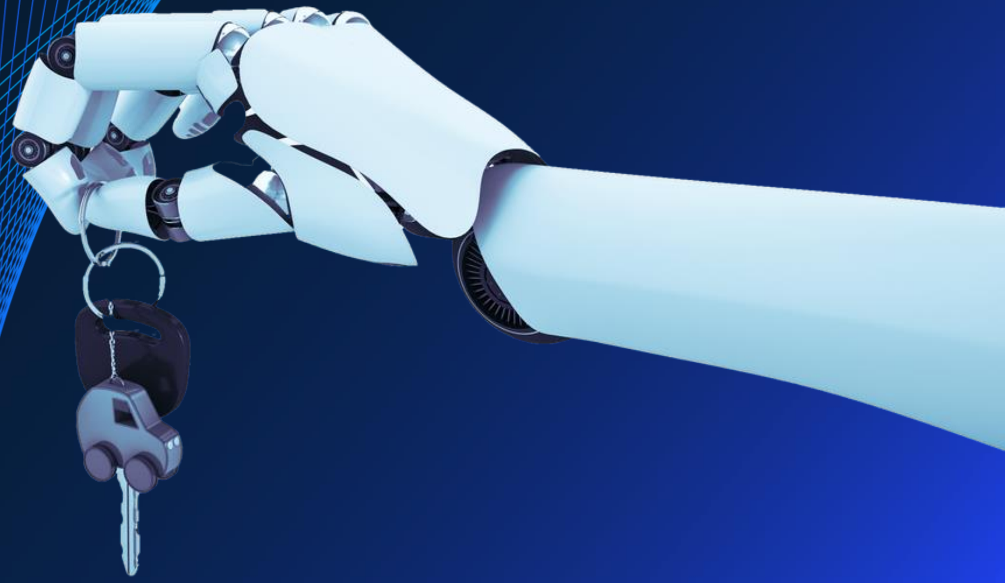
McKinsey
& Company

McKinsey Technology Trends Outlook 2022

Trust architectures and digital identity

August 2022



What is the tech trend about?

Increasing cyberattacks and data breaches continually pose new challenges by leveraging trending technology (eg, quantum computing for encryption breaking). **Digital-trust technologies** empower organizations to gain a competitive advantage by building, scaling, and maintaining the trust of stakeholders (eg, customers, regulators) in the use of their data and digital-enabled products and services.

High-growth technologies[1]

Zero-trust architecture (ZTA)

IT security system design where **all entities,** inside and outside the organization's computer network, **cannot be trusted by default** and need to prove trustworthiness

Includes access management, device protection, network security, data encryption, continuous monitoring, and more

Digital identity

Mechanisms for providing full information that **characterizes** and **distinguishes an individual entity** (eg, system, person, organization) in the digital space

Entities' identities consist of distinguishing **attributes** (eg, name, identifier, characteristics)

Privacy engineering

Techniques used to enable oversight, implementation, operation, and maintenance of privacy

Includes reducing risks to data privacy, resource allocation, and embedding privacy enablement into existing systems

Explainable artificial intelligence (XAI)

Techniques for building **understanding of** and **trust in AI models** for real-world deployment

Addresses fairness, accountability, responsibility, transparency, and ethics

Digital trust addresses digital risk across data, cloud, AI and analytics, and risk culture

[1] Technology areas and specific technologies are not exhaustive of all developments in cybersecurity.

Source: McKinsey analysis

Why should leaders pay attention?

Digital-trust technologies can reduce risk and potential negative impact from cyberattacks

Cyberattacks and cyber regulations are accelerating …

1 out of 3

global organizations experienced a cyberattack in 2019 (+36% vs prior year)

Increasing complexity and frequency of cyberattacks

220×

Increase in spam from Feb−Mar 2020 due to COVID-19 outbreak vulnerabilities

Rising costs and losses from cyberattacks

~$10.5 trillion

Forecast costs and losses related to cybercrime by 2025, representing a 15% annual increase

Growing regulation in the US and globally

+31

New national cyber policies in the US in the past 5 years, with greater numbers globally

… so technology must keep up

$101.5 billion

Projected spending on service providers in digital trust by 2025[1]

3–13%

Predicted economic benefits of digital identity by 2030, expressed as a share of GDP

85%

Share of small and midsize enterprises that intend to increase IT security spending until 2023

~85%

Share of companies that are victims of digital-identity-related fraud each year

[1] Service providers include consultants, hardware support, implementation, and outsourcing.

Source: Center for Strategic International Studies; IBM; Identity Theft Resource Center; Kaspersky Lab; National Cyber Security Centre; PurpleSec data survey; Statista; McKinsey Cyber Market Map, McKinsey Global Institute

Why should leaders pay attention? (continued)

Digital trust offers value creation, enabling organizations to scale faster and become more effective

Increasing opportunities …

- Exponential potential for stacked wins
- Increased speed of digitization
- High potential-market-value advantage
- Better ability to engage in risk reduction

… in a landscape of complications and pitfalls ...

- Increasingly aggressive regulatory scrutiny, resulting in substantial fines and penalties
- Heavy reliance on legacy governance processes and technologies
- Hard-to-understand AI algorithms, which are more complex and less predictable than traditional analytics
- Growing scrutiny from public, media, and watchdog organizations
- Increasing global uncertainty

… leading to economic impact and value

Build a strong foundation of digital trust with customers, enabling increased acquisition

Leverage digital trust to scale internal data and analytic programs sustainably

Advance strategic position for advantage over competitors across AI and analytics, data, cloud, and risk culture

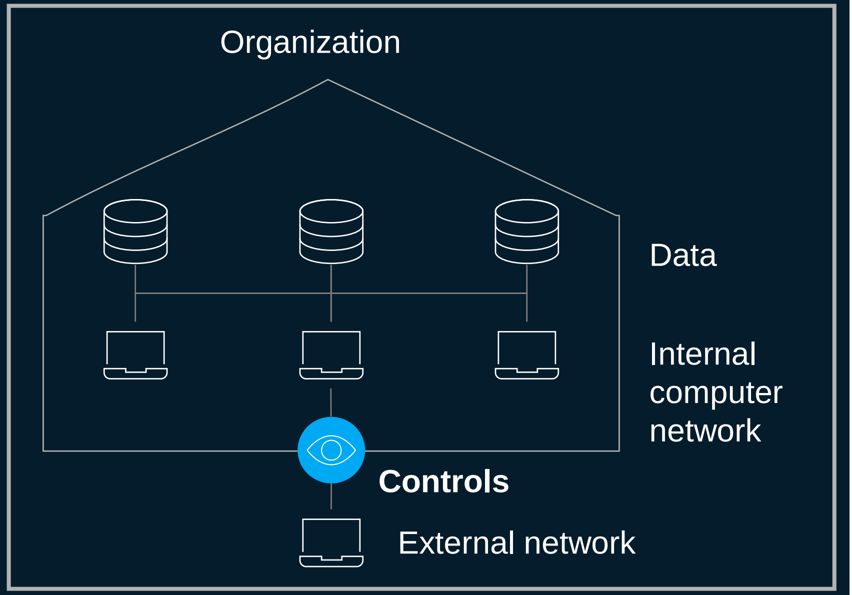
Source: McKinsey analysis

What are the most noteworthy technologies?

Zero-trust architecture assumes “zero trust” for more robust and secure data flow across technical systems

From: Traditional, perimeter-based architecture

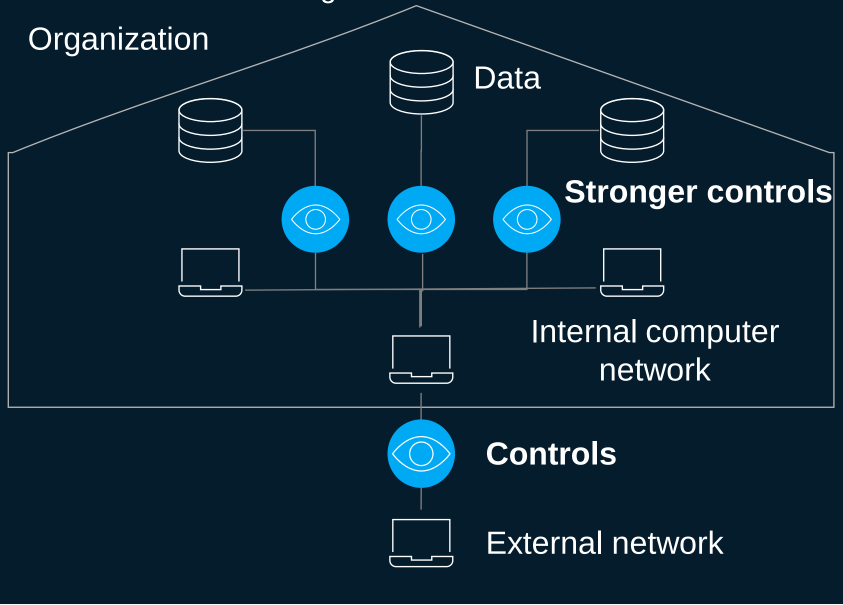
After users are verified and gain access past perimeter controls, **everything within the network is assumed safe**, which does not robustly protect against inner threats



To: Zero-trust architecture

The assumption is that **all entities**, within and outside the organization, **are not to be trusted**

- **Controls** (eg, identity and access management, network controls) are **set up for any interaction by an entity** within the network
- **Strength of controls** depends on **importance and risk level** of protected data and/or asset
- **Network is micro-segmented** to divide data and isolate attacks on data segments



Benefits

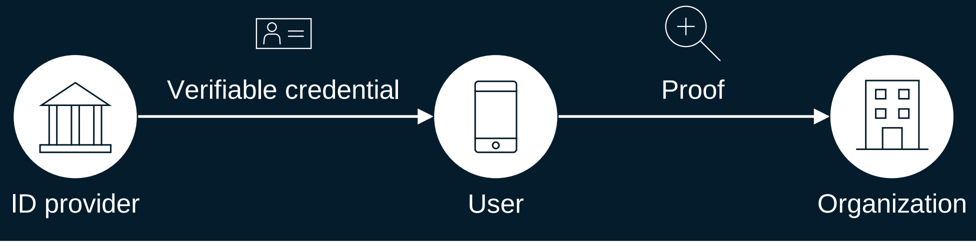
- **Increased security and reduced risk** from increased controls across organizational network and customer data
- **Cost reduction** as losses from cyberattacks decrease
- **Increased visibility and understanding** of user access and traffic across the network from continuous monitoring
- **Upskilled workforce and streamlined technical stack** provide companies with stronger, faster technical capabilities and mitigate technical complexity, priming the company for incorporation of other cybersecurity technologies
- **Improved reputation** (due to fewer breaches in security and stronger technical stack), which can attract customers

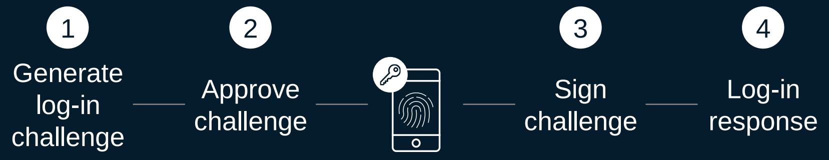
Source: McKinsey analysis

What are the most noteworthy technologies? (continued)

Digital identity is enabling decentralization and new forms of verification – examples of innovation

	Self-sovereign identity (SSI)	‘Passwordless’ identity
Diagram	**Data flow**	**Biometric verification[1]**





	Self-sovereign identity (SSI)	‘Passwordless’ identity
Description	• Users **have control over their verified credentials** (attribute information to identify an individual); they can select the specific data for sharing (eg, name, password) and the sharing audience (eg, employers, healthcare provider)	• Users can verify and authenticate their digital identity without traditional alphanumeric passwords but with other forms of identifying information
Functionality	• Users interact directly with ID issuers and organizations without relying on an intermediary to facilitate data exchange • Data and user credentials are stored on a decentralized ledger (eg, blockchain) for easy access and verification	• Users can provide alternative identifying information, such as: — Biometrics (eg, facial scan, retinal scan, thumbprint, voice) — Devices and apps (eg, mobile phone, email) — Documents (eg, driver’s license, passport)
Benefits	• **Increased individual control** over identity for **trusted transactions without an intermediary;** users themselves control what data they share and with whom from an interoperable and convenient identity source • **Improved security,** because decentralized data storage limits vulnerability to attacks	• **Alternative protections** against rising vulnerability attacks (eg, phishing, brute-force password cracking) • **Reduced inefficiencies** for the user (eg, too many passwords, lost password) • **Efficiency and convenience;** users can rely on streamlined identifying information, based on the level of risk associated with the system

[1] Diagram adapted from Alex Brown, “Passwordless authentication: A complete guide [2022],” Transmit Security, Jan 13, 2022.

Source: Expert input; McKinsey analysis

What are the most noteworthy technologies? (continued)

Privacy engineering governs data privacy protection, while XAI builds trust in AI models

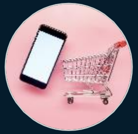
	Privacy engineering	Explainable AI
Description	• Design techniques used to enable the practice governing implementation, operations, and maintenance of privacy • Broadly, these technologies support the strategic reduction of privacy risks, resource allocation, and implementation of privacy controls	• **AI-related techniques combining social science and psychology** to enable people to understand, appropriately trust, and effectively manage emerging AI technologies • Types of “explainability” differ based on the explanation objective (eg, explaining how the model works, clarifying why a model input led to its output, and providing additional information needed for people to trust a model and deploy it)
Benefits	• **Increased safety and control over data** for customers, employees, and organizations, resulting from additional controls and protective measures • **Easier process to implement privacy changes,** because the technologies form a privacy infrastructure that can facilitate privacy updates from the continually evolving regulatory landscape	• **More fair algorithmic outputs** given that XAI technologies can help mitigate bias in the data, model, and other processes • **Increased transparency, confidence, and reliability in AI models,** improving organizational performance, reputation, and relationships • **Improved efficiency and effectiveness across AI model pipeline,** due to greater understanding of model data, inputs, outputs, and algorithms

Source: Alejandro Barredo Arrieta et al., “Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI,” *Information Fusion*, Volume 58, June 2020; Katherine Miller, “Should AI models be explainable? That depends,” Stanford University Human-Centered Artificial Intelligence, Mar 16, 2021; McKinsey analysis

What industries could be most affected by the trend?

Digital-trust technologies could affect all industries leveraging digital technology via **reduced risk**

Information technology and electronics and **financial services** are leading adoption, followed by industries managing highly sensitive and regulated data (eg, healthcare, retail)

Industry affected[1]	Impact from technology trend
Information technology and electronics	• Decreased losses and mitigated risk, because more secure systems (from ZTA and privacy engineering) prevent cyberattacks • Improved software solutions and AI model development and deployment via embedded protocols and controls from privacy engineering and XAI • Enhanced customer experiences and reduced customer friction (eg, easier verification, log-in, etc) through easier, wider options for digital identification • Support of Web3 and metaverse technologies such as digital avatars and blockchain-supported decentralized storage for SSI
Financial services	• Decreased losses and mitigated risk where digital identity verification is crucial for transactions • Pressure on regulators to increase compliance related to digital identity and data sensitivity • Support for decentralized-finance (DeFi) applications (eg, verification for crypto loans)
Healthcare systems and services; pharmaceutical and medical products	• Value created by privacy engineering that balances protection of sensitive healthcare data with development of new uses for these data • Improved secure access to patient medical records; ZTA controls strength of protection, and digital identity can enable a single, unified data source • Advanced development of AI models for healthcare diagnostics, drug design, and treatment, due to greater understanding from XAI
 **Consumer packaged goods and retail**	• Improved secure access to sensitive customer data, enabled by ZTA controls and digital identity • Advanced development of AI models to improve the customer journey and increase revenue, based on greater customer understanding from XAI • Stronger brand reputation, as the technologies encourage stakeholder trust

[1] Not exhaustive; focused on industries leading business adoption.

Source: McKinsey analysis

What industries could be most affected by the trend? (continued)

Digital-trust technologies could affect all industries leveraging digital technology via **reduced risk.**

The following industries also demonstrate high value-creation potential from digital-trust technologies.

Industry affected	Impact from technology trend
Aerospace and defense	• Prevent data breaches that could threaten national security and classified information
Education	• Protect students' digital identity and data while ensuring access to educational resources
Media and entertainment	• Protect intellectual property and media content across a fragmented industry value chain dependent on flows of consumer and sensitive data
Public and social sectors	• Enable expansion of digital service opportunities • Secure and verify digital identity in addition to privacy engineering to protect citizen data
Telecommun-ications	• Build digital-identity services on next-generation networks to expand their offerings • Enable enhanced customer experience • Ensure security of 3rd-party partners on their networks • Apply ZTAs and privacy engineering to internal systems and processes

Source: McKinsey analysis

What should leaders consider when engaging with the trend?

Zero-trust architecture

Long-term effort with incremental progress

Effective and full-fledged ZTA, privacy engineering, and XAI cannot be implemented immediately; for reliable results, organizations should gradually increase their controls and test them

Performance efficiency and scalability

Added authentication steps (eg, secure communications using VPN and public key infrastructure [PKI]) can slow daily work and network efficiency; this can vary based on the frequency of controls and size of the network

Privacy engineering

Inherent tension between privacy and fairness

Privacy and fairness can conflict: privacy approaches could restrict collection of personal data, while fairness approaches would collect personal data to detect bias

Digital identity

Nascent ecosystem

SSI has relatively few standards available, and Web3 is a rapidly growing space

Various dependencies

Progress depends on use of existing standards and infrastructures (eg, data regulations) and on development of rising technologies; registering alternative verified credentials can also be a complex process

Concerns over privacy of biometric data

Control, storage, and use of biometric data is a debated topic regarding privacy and ethics

Explainable AI

Lack of standardization

Deciphering the “black box” of large AI models to provide a meaningful explanation is challenging and depends on the task; resulting solutions could face new or unaddressed risks and need to balance privacy, fairness, accountability, responsibility, transparency, and ethics

Overarching risks and uncertainties

Implementation complexity will be significant given resource requirements, talent scarcity, lack of shared taxonomies, coordination challenges across multiple parties, and required shifts in organizational norms and practices needed to achieve effective deployments

Compatibility challenges will be encountered when updating or migrating technologies and integrating them with legacy systems or with an abundance of fragmented point solutions

Evolving regulations involving digital trust and privacy have become a prominent topic, as past standards (eg, on data privacy and data permanency) conflict with these technologies; regulatory measures to reconcile these differences and define newer areas will influence the direction of digital trust

Tensions between privacy and fairness can arise, for example, tension between the avoidance of excessive collection of demographic data and the need for that data to assess and mitigate bias

Lack of standardization and widely accepted best practices for how or when to use trust architecture techniques across industries will continue to be a challenge

Source: McKinsey analysis

Who has successfully created impact with trust architectures and digital identity?

Zero-trust architecture

A **Latin American oil and gas company** with a small IT estate began maturing its capabilities before establishing a ZTA rollout plan; rollout of the security update occurred on a system-by-system basis, targeting high-risk assets first, with the first full ZTA proof of concept implemented 1 year following rollout start date

Self-sovereign identity

BankID is a digital-identification service providing users in Sweden a single source of ID through their mobile phones; with BankID, users can make payments, participate in financial services, log in to government platforms, and access their medical records.

Passwordless identity

Apple has been working toward passwordless sign-ins, such as with Touch ID (ie, thumbprint) and Face ID (ie, facial recognition); As of May 2022, numerous technology companies and service providers, including Google and Microsoft, are working with the FIDO Alliance and World Wide Web Consortium to support passwordless sign-in standards

Source: Company websites; McKinsey analysis

What are some topics of debate related to the trend?

Development of digital trust depends on other trending technologies and the overall ecosystem, raising questions about its path forward.

1 Stakeholder expectations

How are the expectations of customers, employees, and communities changing in terms of data (especially privacy), transparency and outcomes of analytics, and technology security and resilience?

As new technologies seek to personalize the user experience, stakeholders will expect a balance between privacy (a priority that calls for not collecting demographic data) and fairness (a priority that can use demographic data to test for and correct biases). In one study, 97% of people surveyed expressed concern that businesses and the government might misuse their data.[1]

2 Data and privacy regulation

How do regulators reconcile past standards with rising technologies that have inherent conflicts?

Existing data privacy regulations can be at odds with emerging Web3 technologies. For example, the “right to be forgotten” from the General Data Protection Regulation in the EU enforces people’s right to have their data deleted. Storing data on the blockchain, however, creates the potential for an immutable ledger from which past data cannot be “deleted.”

3 Risk area identification

Where are companies typically most exposed to digital and analytics risk?

Improperly-decommissioned legacy systems, breaches to 3rd-party partners, and poorly configured database links, for example, are vulnerabilities that hackers can exploit. The right risk-management approach will require companies to define a mature enterprise-risk framework and conduct formal, holistic risk assessments tailored to their individual systems.

[1] Theodore Forbath et al., “Customer data: Designing for transparency and trust,” *Harvard Business Review,* May 2015.

Additional resources

Knowledge centers

[McKinsey Risk and Resilience Practice]

[McKinsey Technology: Cybersecurity]

Related reading

[Getting to know—and manage—your biggest AI risks]

[Derisking digital and analytics transformations]

[Cybersecurity trends: Looking over the horizon]