

# Digital Trust & Cybersecurity Market Forecasts to 2032 – Global Analysis By Component (Solutions, Services), Digital Identity Type, Deployment Model, Organization Size, End User and By Geography

<https://marketpublishers.com/r/D3F82ADB054FEN.html>

Date: April 2025

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: D3F82ADB054FEN

## Abstracts

According to Statistics MRC, the Global Digital Trust & Cybersecurity Market is accounted for \$386.1 billion in 2025 and is expected to reach \$875.1 billion by 2032 growing at a CAGR of 12.4% during the forecast period. Digital Trust is the confidence that individuals and organizations have in the reliability, integrity, and security of digital systems and interactions. It ensures that data is handled ethically, privacy is respected, and online services function as promised, fostering seamless, secure digital experiences. Cybersecurity, closely intertwined, refers to the technologies, processes, and practices designed to protect computers, networks, and data from unauthorized access, attacks, or damage. Together, they form the foundation of a safe digital ecosystem, where businesses and users can interact without fear of breaches or manipulation, enabling trust, innovation, and the continued growth of the digital economy.

### Market Dynamics:

Driver:

#### Surge in Cybersecurity Threats

The escalating frequency and sophistication of cyberattacks are driving unprecedented demand for robust cybersecurity solutions. As digital ecosystems expand, threats like ransomware, phishing, and data breaches pose serious risks to businesses and individuals. This surge compels organizations to invest in advanced security

frameworks, boosting market growth. The increasing reliance on cloud services, IoT, and remote work further amplifies vulnerabilities, making cybersecurity a top priority across sectors and fueling the digital trust and cybersecurity market.

Restraint:

#### Shortage of Skilled Professionals

Despite growing demand, the cybersecurity industry faces a critical shortage of skilled professionals. Organizations struggle to recruit talent with expertise in threat detection, risk management, and compliance. This talent gap hampers the implementation of effective security strategies and slows innovation. As cyber threats evolve, the lack of qualified personnel limits the scalability of solutions and increases operational risks, posing a major restraint to market expansion and the realization of secure digital environments.

Opportunity:

#### Digital Transformation Across Sectors

The global push for digital transformation presents a massive opportunity for the digital trust and cybersecurity market. Industries such as healthcare, finance, and manufacturing are rapidly adopting digital platforms, cloud computing, and AI-driven systems. This shift demands secure, trustworthy digital infrastructures to protect sensitive data and ensure regulatory compliance. As businesses modernize, the need for integrated cybersecurity and digital trust solutions grows, unlocking new revenue streams and accelerating market growth across diverse verticals.

Threat:

#### High Cost of Compliance and Implementation

Implementing comprehensive cybersecurity frameworks and maintaining compliance with evolving regulations can be prohibitively expensive. Small and medium enterprises often struggle with the financial burden of deploying advanced security technologies and hiring specialized staff. Additionally, frequent updates to global data protection laws increase complexity and cost. These financial and operational challenges may deter adoption, especially in emerging markets, posing a significant threat to the widespread implementation.

## Covid-19 Impact

The COVID-19 pandemic reshaped digital landscapes, accelerating remote work and cloud adoption. While this created new opportunities, it also exposed vulnerabilities in existing cybersecurity infrastructures. Organizations faced increased cyber threats, from phishing attacks to ransomware targeting remote employees. The crisis highlighted the importance of digital trust, prompting urgent investments in secure communication tools and identity management systems.

The centralized identity segment is expected to be the largest during the forecast period

The centralized identity segment is expected to account for the largest market share during the forecast period, due to its streamlined management and control over user credentials. Centralized systems offer simplicity and efficiency in authentication processes, making them ideal for large enterprises and government agencies. Their ability to enforce consistent security policies and monitor access across platforms enhances trust and reduces risk. As organizations prioritize secure identity frameworks, centralized identity solutions remain the backbone of digital trust strategies.

The federated identity segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the federated identity segment is predicted to witness the highest growth rate, due to growing need for seamless, secure access across multiple platforms. This model allows users to authenticate through a single identity provider across various services, improving user experience and reducing password fatigue. Its scalability and interoperability make it attractive for cloud-based applications and collaborative environments. As digital ecosystems become more interconnected, federated identity solutions offer a flexible, secure alternative to traditional identity management.

### **Region with largest share:**

During the forecast period, the Asia Pacific region is expected to hold the largest market share due to rapid digitalization, expanding internet penetration, and growing investments in cybersecurity infrastructure. Countries like China, India, and Japan are witnessing a surge in digital services, e-commerce, and fintech, necessitating robust security frameworks. Government initiatives promoting digital trust and data protection

further fuel market growth. The region's dynamic tech landscape and increasing awareness of cyber threats position it as a dominant force in the global market.

### **Region with highest CAGR:**

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR, owing to advanced technological adoption and stringent regulatory frameworks. The region's mature cybersecurity ecosystem, coupled with rising cybercrime incidents, propels demand for innovative solutions. Investments in AI, blockchain, and zero-trust architectures enhance digital trust capabilities. Additionally, strong government support and a thriving startup culture contribute to rapid growth. North America's proactive approach to digital security positions it as a key accelerator in the global market.

### **Key players in the market**

Some of the key players profiled in the Digital Trust & Cybersecurity Market include Palo Alto Networks, Amazon Web Services (AWS), CrowdStrike, Thales Group, Cisco Systems, Oracle Corporation, Check Point Software Technologies, Salesforce, Fortinet, RSA Security, IBM Corporation, DigiCert, Microsoft Corporation, Zscaler and Trend Micro

### **Key Developments:**

In September 2025, Microsoft Fabric Community Conference (FabCon), Microsoft unveiled major upgrades to its Fabric platform, including new Graph and Maps capabilities. These enhancements support deeper AI readiness and data contextualization, enabling organizations to build smarter agents and applications.

In September 2025, Workday announced a strategic collaboration with Microsoft to integrate AI agents built using Microsoft Azure AI Foundry and Copilot Studio into Workday's Agent System of Record (ASOR). This partnership aims to streamline enterprise AI management by verifying agent identity and ensuring secure, context-aware operations across business systems.

### **Components Covered:**

Solutions

Services

#### Digital Identity Types Covered:

Centralized Identity

Federated Identity

Decentralized Identity

#### Deployment Models Covered:

On-Premises

Cloud-Based

Hybrid

#### Organization Sizes Covered:

Large Enterprises

Small & Medium Enterprises (SMEs)

#### End Users Covered:

Banking, Financial Services & Insurance (BFSI)

Healthcare & Life Sciences

Information Technology & Telecommunications

Government & Public Sector

Retail & E-Commerce

Energy & Utilities

Others End Users

Regions Covered:

North America

US

Canada

Mexico

Europe

Germany

UK

Italy

France

Spain

Rest of Europe

Asia Pacific

Japan

China

India

Australia

New Zealand

South Korea

Rest of Asia Pacific

South America

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

**What our report offers:**

- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments

- Supply chain trends mapping the latest technological advancements

### **Free Customization Offerings:**

All the customers of this report will be entitled to receive one of the following free customization options:

#### Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

#### Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

#### Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

## Contents

### **1 EXECUTIVE SUMMARY**

### **2 PREFACE**

- 2.1 Abstract
- 2.2 Stake Holders
- 2.3 Research Scope
- 2.4 Research Methodology
  - 2.4.1 Data Mining
  - 2.4.2 Data Analysis
  - 2.4.3 Data Validation
  - 2.4.4 Research Approach
- 2.5 Research Sources
  - 2.5.1 Primary Research Sources
  - 2.5.2 Secondary Research Sources
  - 2.5.3 Assumptions

### **3 MARKET TREND ANALYSIS**

- 3.1 Introduction
- 3.2 Drivers
- 3.3 Restraints
- 3.4 Opportunities
- 3.5 Threats
- 3.6 End User Analysis
- 3.7 Emerging Markets
- 3.8 Impact of Covid-19

### **4 PORTERS FIVE FORCE ANALYSIS**

- 4.1 Bargaining power of suppliers
- 4.2 Bargaining power of buyers
- 4.3 Threat of substitutes
- 4.4 Threat of new entrants
- 4.5 Competitive rivalry

### **5 GLOBAL DIGITAL TRUST & CYBERSECURITY MARKET, BY COMPONENT**

## 5.1 Introduction

## 5.2 Solutions

### 5.2.1 Identity & Access Management (IAM)

### 5.2.2 Digital Signatures & Certificates

### 5.2.3 Public Key Infrastructure (PKI)

### 5.2.4 Blockchain & Distributed Ledger Technologies

### 5.2.5 Data Encryption & Security

## 5.3 Services

### 5.3.1 Consulting & Integration

### 5.3.2 Support & Maintenance

### 5.3.3 Managed Services

## **6 GLOBAL DIGITAL TRUST & CYBERSECURITY MARKET, BY DIGITAL IDENTITY TYPE**

### 6.1 Introduction

### 6.2 Centralized Identity

### 6.3 Federated Identity

### 6.4 Decentralized Identity

## **7 GLOBAL DIGITAL TRUST & CYBERSECURITY MARKET, BY DEPLOYMENT MODEL**

### 7.1 Introduction

### 7.2 On-Premises

### 7.3 Cloud-Based

### 7.4 Hybrid

## **8 GLOBAL DIGITAL TRUST & CYBERSECURITY MARKET, BY ORGANIZATION SIZE**

### 8.1 Introduction

### 8.2 Large Enterprises

### 8.3 Small & Medium Enterprises (SMEs)

## **9 GLOBAL DIGITAL TRUST & CYBERSECURITY MARKET, BY END USER**

### 9.1 Introduction

- 9.2 Banking, Financial Services & Insurance (BFSI)
- 9.3 Healthcare & Life Sciences
- 9.4 Information Technology & Telecommunications
- 9.5 Government & Public Sector
- 9.6 Retail & E-Commerce
- 9.7 Energy & Utilities
- 9.8 Others End Users

## **10 GLOBAL DIGITAL TRUST & CYBERSECURITY MARKET, BY GEOGRAPHY**

- 10.1 Introduction
- 10.2 North America
  - 10.2.1 US
  - 10.2.2 Canada
  - 10.2.3 Mexico
- 10.3 Europe
  - 10.3.1 Germany
  - 10.3.2 UK
  - 10.3.3 Italy
  - 10.3.4 France
  - 10.3.5 Spain
  - 10.3.6 Rest of Europe
- 10.4 Asia Pacific
  - 10.4.1 Japan
  - 10.4.2 China
  - 10.4.3 India
  - 10.4.4 Australia
  - 10.4.5 New Zealand
  - 10.4.6 South Korea
  - 10.4.7 Rest of Asia Pacific
- 10.5 South America
  - 10.5.1 Argentina
  - 10.5.2 Brazil
  - 10.5.3 Chile
  - 10.5.4 Rest of South America
- 10.6 Middle East & Africa
  - 10.6.1 Saudi Arabia
  - 10.6.2 UAE
  - 10.6.3 Qatar

10.6.4 South Africa

10.6.5 Rest of Middle East & Africa

## **11 KEY DEVELOPMENTS**

11.1 Agreements, Partnerships, Collaborations and Joint Ventures

11.2 Acquisitions & Mergers

11.3 New Product Launch

11.4 Expansions

11.5 Other Key Strategies

## **12 COMPANY PROFILING**

12.1 Palo Alto Networks

12.2 Amazon Web Services (AWS)

12.3 CrowdStrike

12.4 Thales Group

12.5 Cisco Systems

12.6 Oracle Corporation

12.7 Check Point Software Technologies

12.8 Salesforce

12.9 Fortinet

12.10 RSA Security

12.11 IBM Corporation

12.12 DigiCert

12.13 Microsoft Corporation

12.14 Zscaler

12.15 Trend Micro

## List Of Tables

### LIST OF TABLES

Table 1 Global Digital Trust & Cybersecurity Market Outlook, By Region (2024-2032) (\$MN)

Table 2 Global Digital Trust & Cybersecurity Market Outlook, By Component (2024-2032) (\$MN)

Table 3 Global Digital Trust & Cybersecurity Market Outlook, By Solutions (2024-2032) (\$MN)

Table 4 Global Digital Trust & Cybersecurity Market Outlook, By Identity & Access Management (IAM) (2024-2032) (\$MN)

Table 5 Global Digital Trust & Cybersecurity Market Outlook, By Digital Signatures & Certificates (2024-2032) (\$MN)

Table 6 Global Digital Trust & Cybersecurity Market Outlook, By Public Key Infrastructure (PKI) (2024-2032) (\$MN)

Table 7 Global Digital Trust & Cybersecurity Market Outlook, By Blockchain & Distributed Ledger Technologies (2024-2032) (\$MN)

Table 8 Global Digital Trust & Cybersecurity Market Outlook, By Data Encryption & Security (2024-2032) (\$MN)

Table 9 Global Digital Trust & Cybersecurity Market Outlook, By Services (2024-2032) (\$MN)

Table 10 Global Digital Trust & Cybersecurity Market Outlook, By Consulting & Integration (2024-2032) (\$MN)

Table 11 Global Digital Trust & Cybersecurity Market Outlook, By Support & Maintenance (2024-2032) (\$MN)

Table 12 Global Digital Trust & Cybersecurity Market Outlook, By Managed Services (2024-2032) (\$MN)

Table 13 Global Digital Trust & Cybersecurity Market Outlook, By Digital Identity Type (2024-2032) (\$MN)

Table 14 Global Digital Trust & Cybersecurity Market Outlook, By Centralized Identity (2024-2032) (\$MN)

Table 15 Global Digital Trust & Cybersecurity Market Outlook, By Federated Identity (2024-2032) (\$MN)

Table 16 Global Digital Trust & Cybersecurity Market Outlook, By Decentralized Identity (2024-2032) (\$MN)

Table 17 Global Digital Trust & Cybersecurity Market Outlook, By Deployment Model (2024-2032) (\$MN)

Table 18 Global Digital Trust & Cybersecurity Market Outlook, By On-Premises

(2024-2032) (\$MN)

Table 19 Global Digital Trust & Cybersecurity Market Outlook, By Cloud-Based

(2024-2032) (\$MN)

Table 20 Global Digital Trust & Cybersecurity Market Outlook, By Hybrid (2024-2032)

(\$MN)

Table 21 Global Digital Trust & Cybersecurity Market Outlook, By Organization Size

(2024-2032) (\$MN)

Table 22 Global Digital Trust & Cybersecurity Market Outlook, By Large Enterprises

(2024-2032) (\$MN)

Table 23 Global Digital Trust & Cybersecurity Market Outlook, By Small & Medium Enterprises (SMEs) (2024-2032) (\$MN)

Table 24 Global Digital Trust & Cybersecurity Market Outlook, By End User (2024-2032)

(\$MN)

Table 25 Global Digital Trust & Cybersecurity Market Outlook, By Banking, Financial Services & Insurance (BFSI) (2024-2032) (\$MN)

Table 26 Global Digital Trust & Cybersecurity Market Outlook, By Healthcare & Life Sciences (2024-2032) (\$MN)

Table 27 Global Digital Trust & Cybersecurity Market Outlook, By Information Technology & Telecommunications (2024-2032) (\$MN)

Table 28 Global Digital Trust & Cybersecurity Market Outlook, By Government & Public Sector (2024-2032) (\$MN)

Table 29 Global Digital Trust & Cybersecurity Market Outlook, By Retail & E-Commerce (2024-2032) (\$MN)

Table 30 Global Digital Trust & Cybersecurity Market Outlook, By Energy & Utilities (2024-2032) (\$MN)

Table 31 Global Digital Trust & Cybersecurity Market Outlook, By Others End Users (2024-2032) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

## I would like to order

Product name: Digital Trust & Cybersecurity Market Forecasts to 2032 – Global Analysis By Component (Solutions, Services), Digital Identity Type, Deployment Model, Organization Size, End User and By Geography

Product link: <https://marketpublishers.com/r/D3F82ADB054FEN.html>

Price: US\$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/D3F82ADB054FEN.html>