

CEG7560

---



# Cyber Security and Data Science Trends

# Cyber Security Trends

---

## Cybersecurity trends: Looking over the horizon

McKinsey, March 10, 2022

<https://www.mckinsey.com/cybersecurity/cybersecurity-trends-looking-over-the-horizon>

# Cyber Security Trends

---

- Cyber security is a never ending race
- Both sides constantly increase their efforts
- As number of attacks increases, defense mechanisms have to improve

# Cyber Security Trends

Cyberattacks are on the rise, and market indicators reflect a fear of further increases.

Future outlook of cybersecurity market



**\$101.5**

billion in projected  
spending on  
service providers<sup>1</sup>  
by 2025



**15%**

annual increase of  
costs related  
to cybercrime; will  
reach **\$10.5 trillion** a  
year in 2025



**85%**

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



**3.5**

million  
cybersecurity  
positions now  
open worldwide



**+21%**

forecast of com-  
pound annual growth  
for direct cyber  
insurance  
premiums until 2025

<sup>1</sup>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; press; PurpleSec data survey; Statista; McKinsey Cyber Market Map

McKinsey  
& Company

# Cyber Security Trends

---

Three cybersecurity trends with large-scale implications:

- On-demand access to ubiquitous data and information platforms is growing
- Hackers are using AI, machine learning, and other technologies to launch increasingly sophisticated attacks
- Ever-growing regulatory landscape and continued gaps in resources, knowledge, and talent will outpace cybersecurity

# Cyber Security Trends

---

Responses to trend one:

- Zero trust architecture: Bring your own device (BYOD) requires that devices may not be trusted
- Behavioral analytics: Anomaly detection, monitoring of access, health of devices
- Elastic log monitoring for large data sets: Real-time visualization and analysis of the data
- Encryption

# Cyber Security Trends

---

Responses to trend two:

- Automation implemented through a risk-based approach: Automated patching, configuration, and software upgrades
- Use of defensive AI and machine learning for cybersecurity: Detect outlier patterns and remediate noncompliant systems
- Technical and organizational responses to ransomware: Use of resilient data repositories and infrastructure, automated responses to malicious encryption, and advanced multifactor authentication

# Cyber Security Trends

---

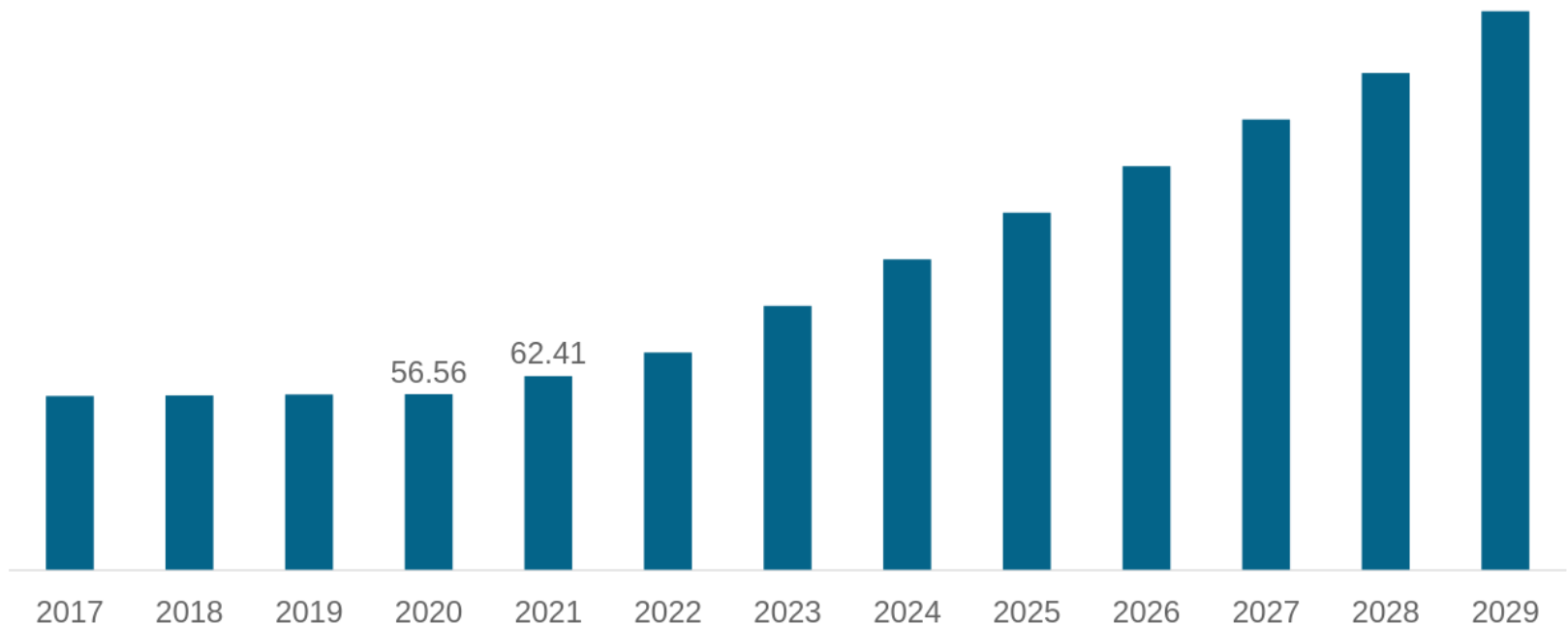
Responses to trend three:

- Secure software development: Create a secure software development life cycle
- Taking advantage of X as a service: Cloud providers not only handle many routine security, patching, and maintenance activities but also offer automation capabilities and scalable services
- Infrastructure and security as code: Use of standardizing and codifying infrastructure and control-engineering processes
- Software bill of materials: Detailing all components and supply chain relationships used in software to achieve compliance



# Cyber Security Trends

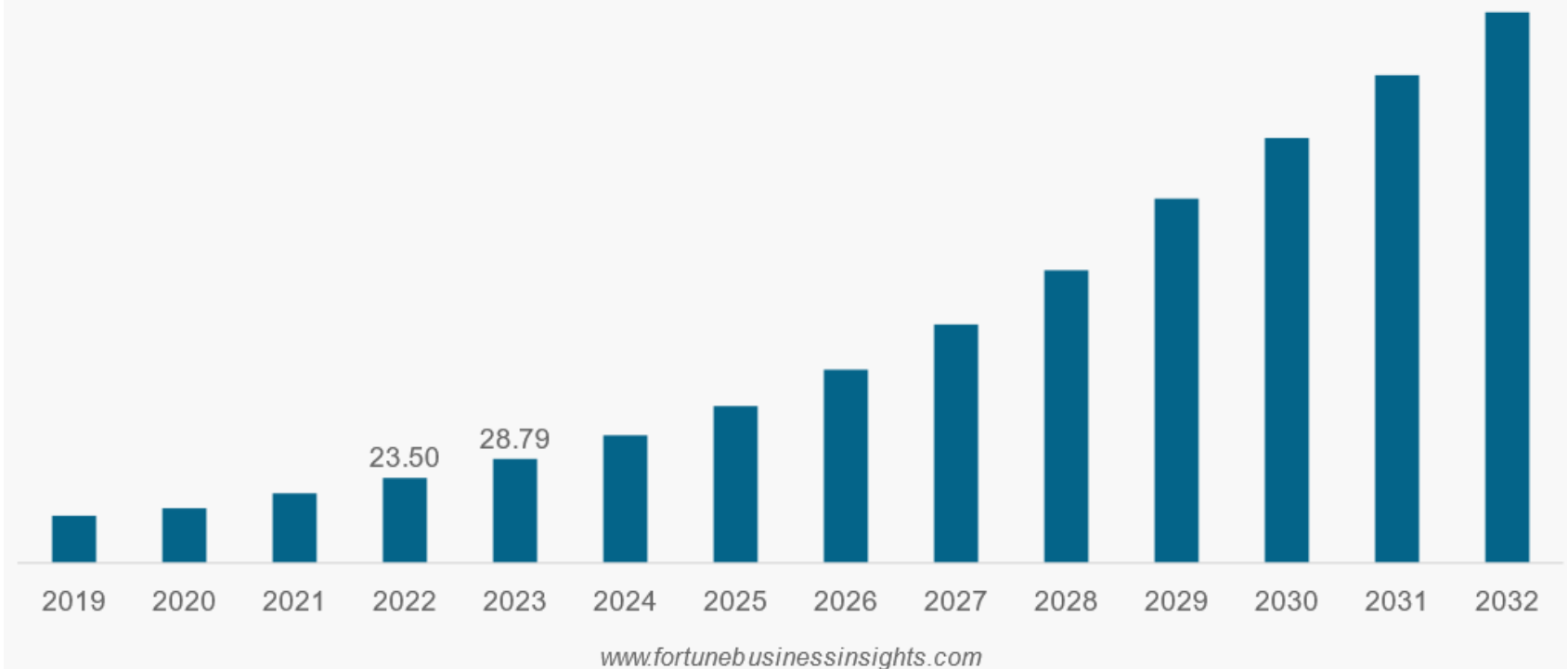
North America Cyber Security Market Size, 2018-2029 (USD Billion)



[www.fortunebusinessinsights.com](http://www.fortunebusinessinsights.com)

# Data Science Trends

North America Data Science Platform Market Size, 2019-2032 (USD Billion)



# Cyber Security and Data Science Trends

---

Visualization opportunities:

- Data analytics/visual analytics
- Tackling large-scale data problem
  - Lots of data is generated in terms of
    - Network traffic
    - Log files
    - ...
- Sanity check for AI (XAI, verifying decisions, ...)
- Human-in-the-loop
- Additional safe-guard to automated systems
- Forensic analysis after an attack