CEG7560

Cyber Security and Data Science Trends

Cyber Security Trends

Cybersecurity trends: Looking over the horizon

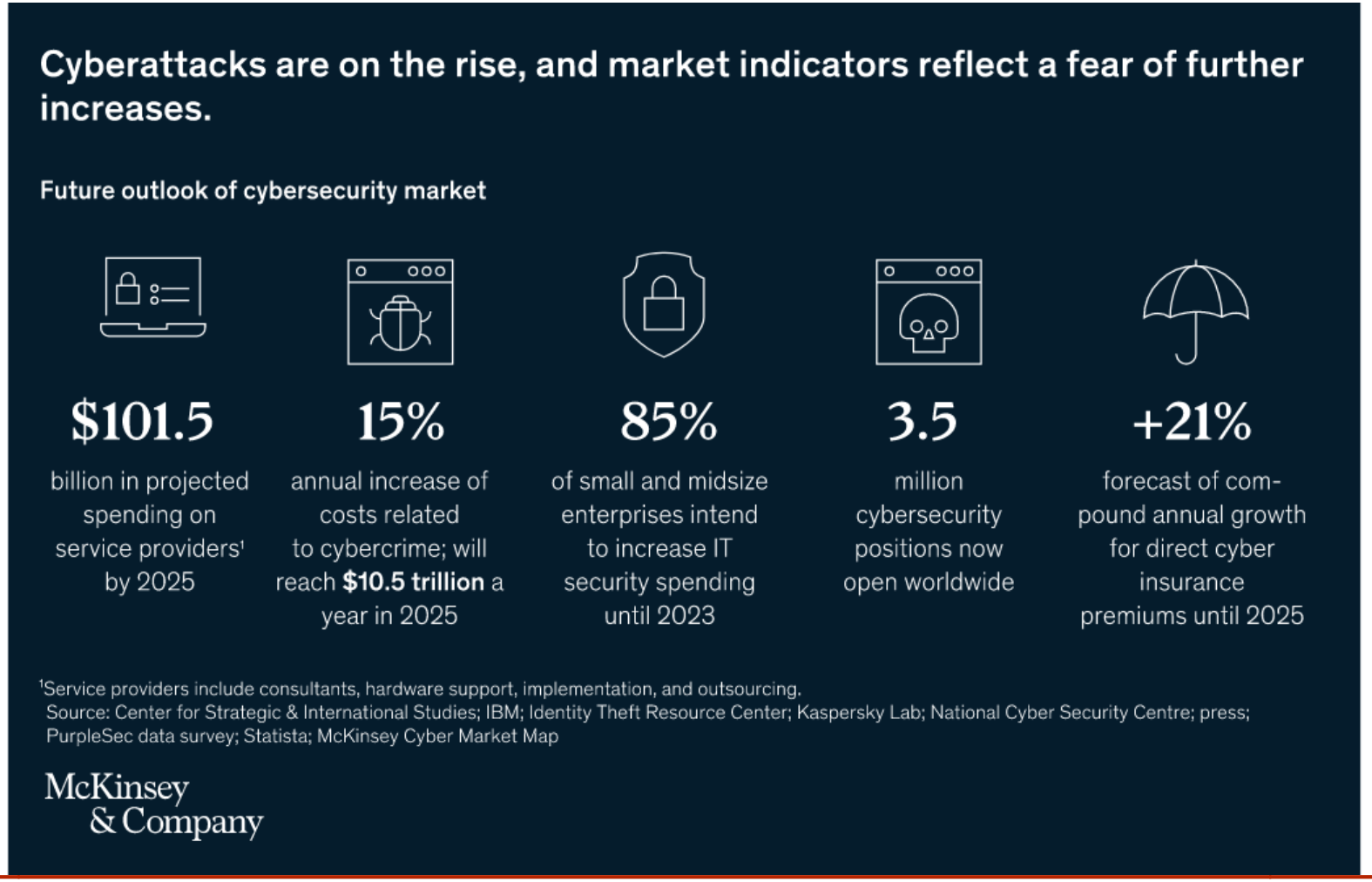
McKinsey, March 10, 2022

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



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:

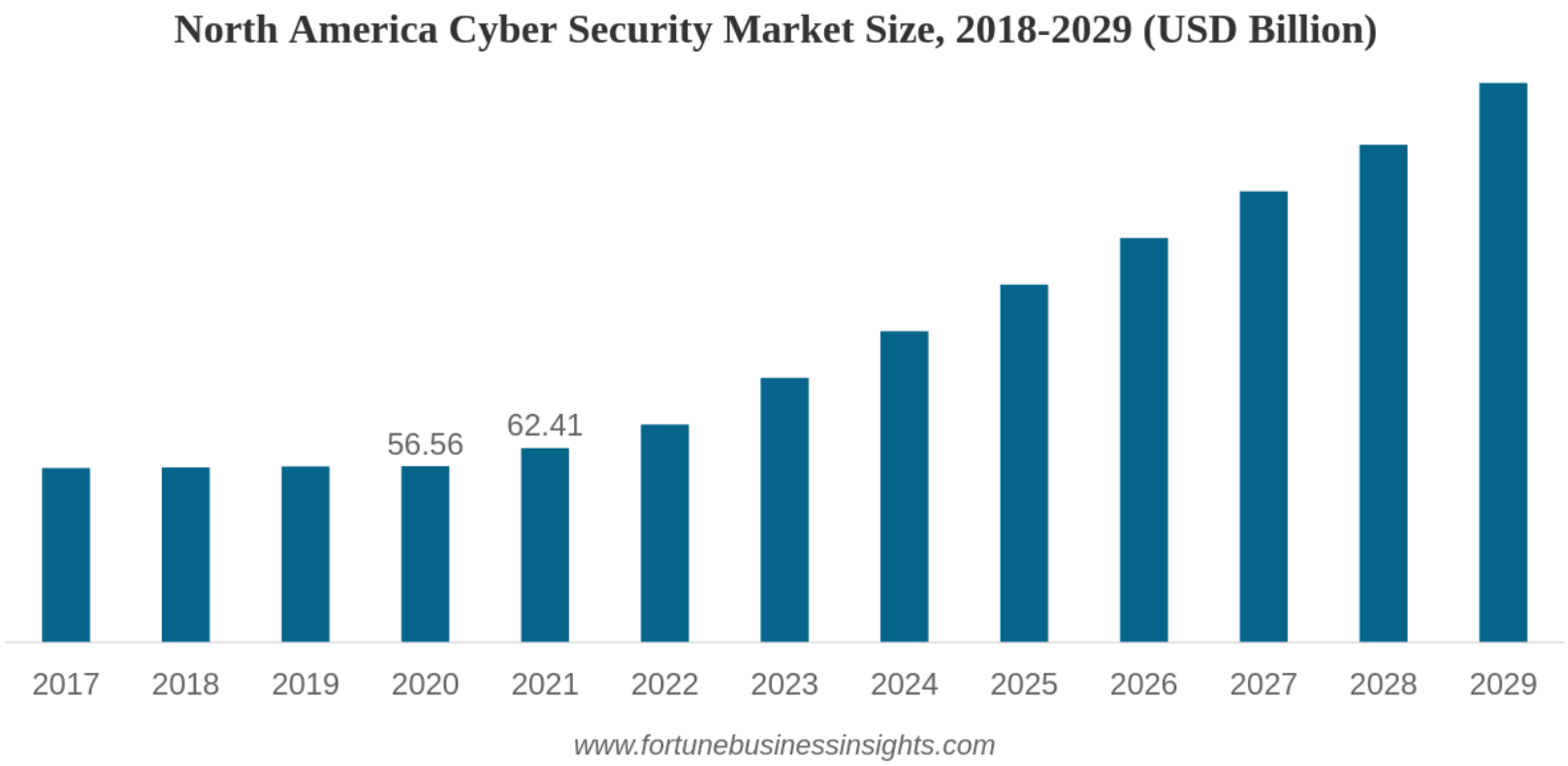
- Automation implemented through a risk-based approach: Automated patching, configuration, and software upgrades
- Use of defensive AI and machine learning for cybersecurity: Detect outlier patterns and remediate noncompliant systems
- Technical and organizational responses to ransomware: Use of resilient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

Cyber Security Trends

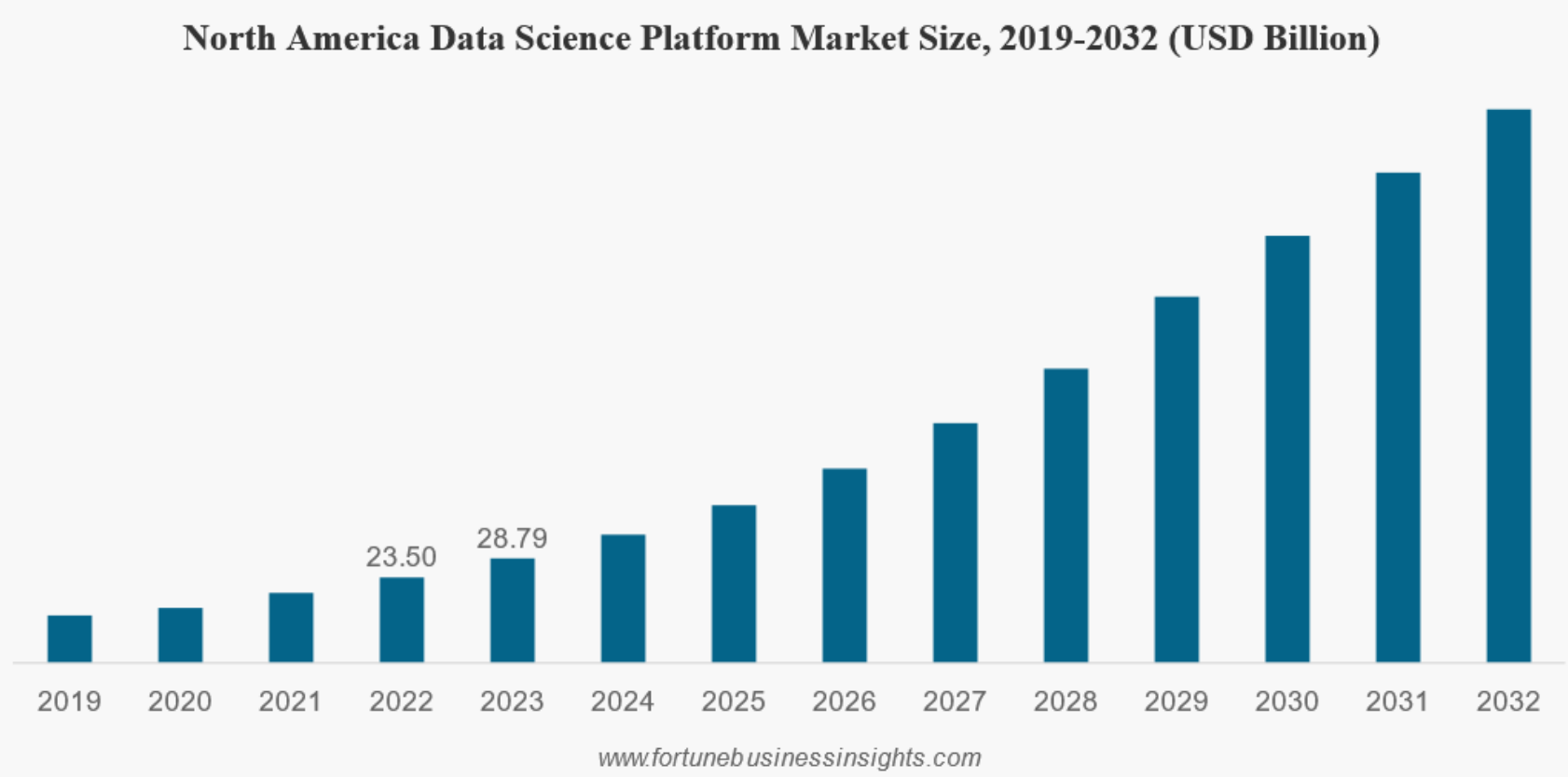
Responses to trend three:

- 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 complience

Cyber Security Trends



Data Science Trends



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