

A Guide to Security in Software Development



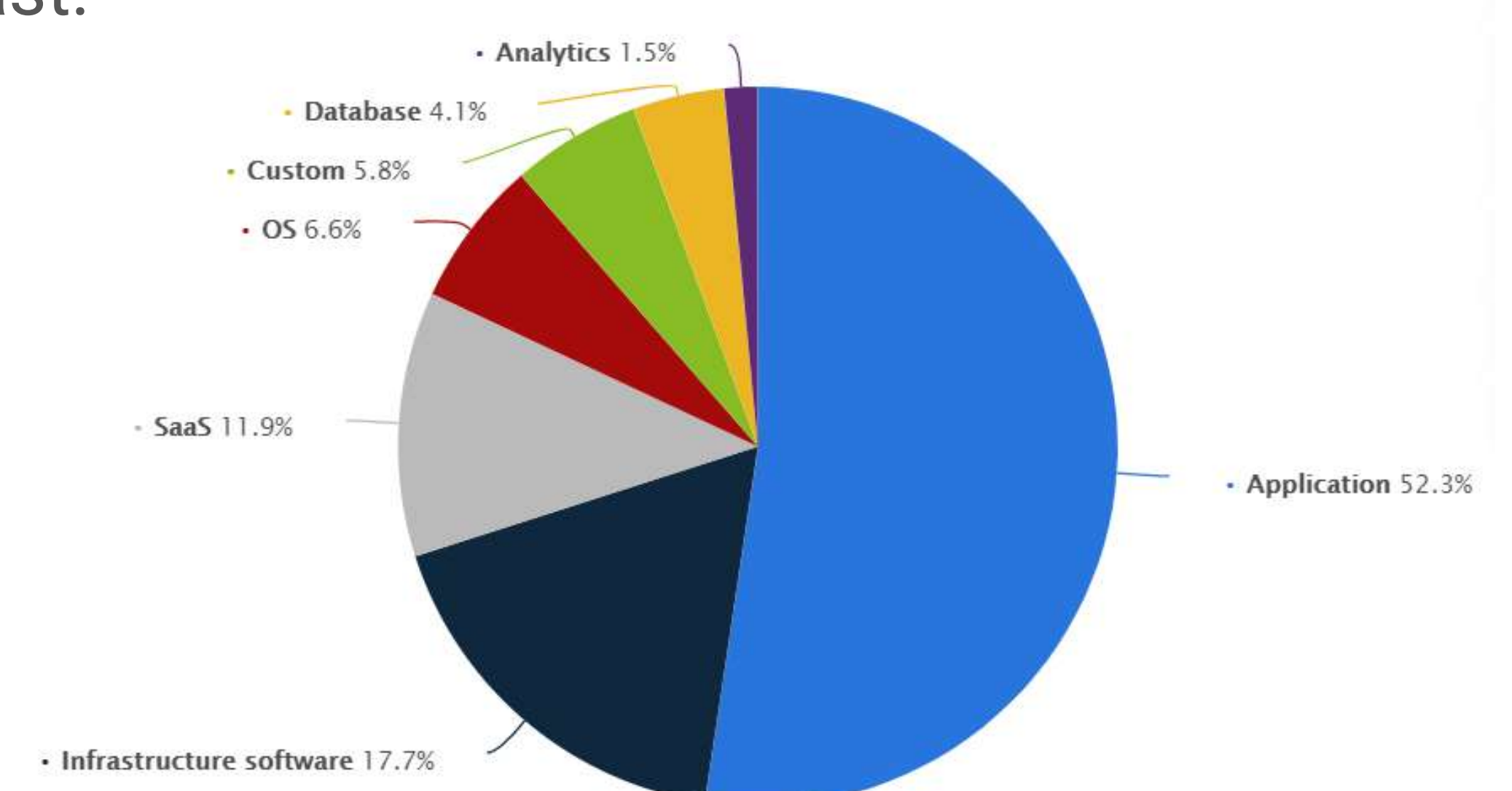
Matching the changing pace of technologies and prospering the growth is the new face of business survival. Every passing day leads us to more advanced and trailblazing aspects of lifestyle through pioneering software development. From online shopping to taking online classes, from artificial intelligence to cryptocurrency, everything revolves around the digital ecosystem. Every effort of developers and programmers is to cater a soothing and hassle-free digital experience to every user.

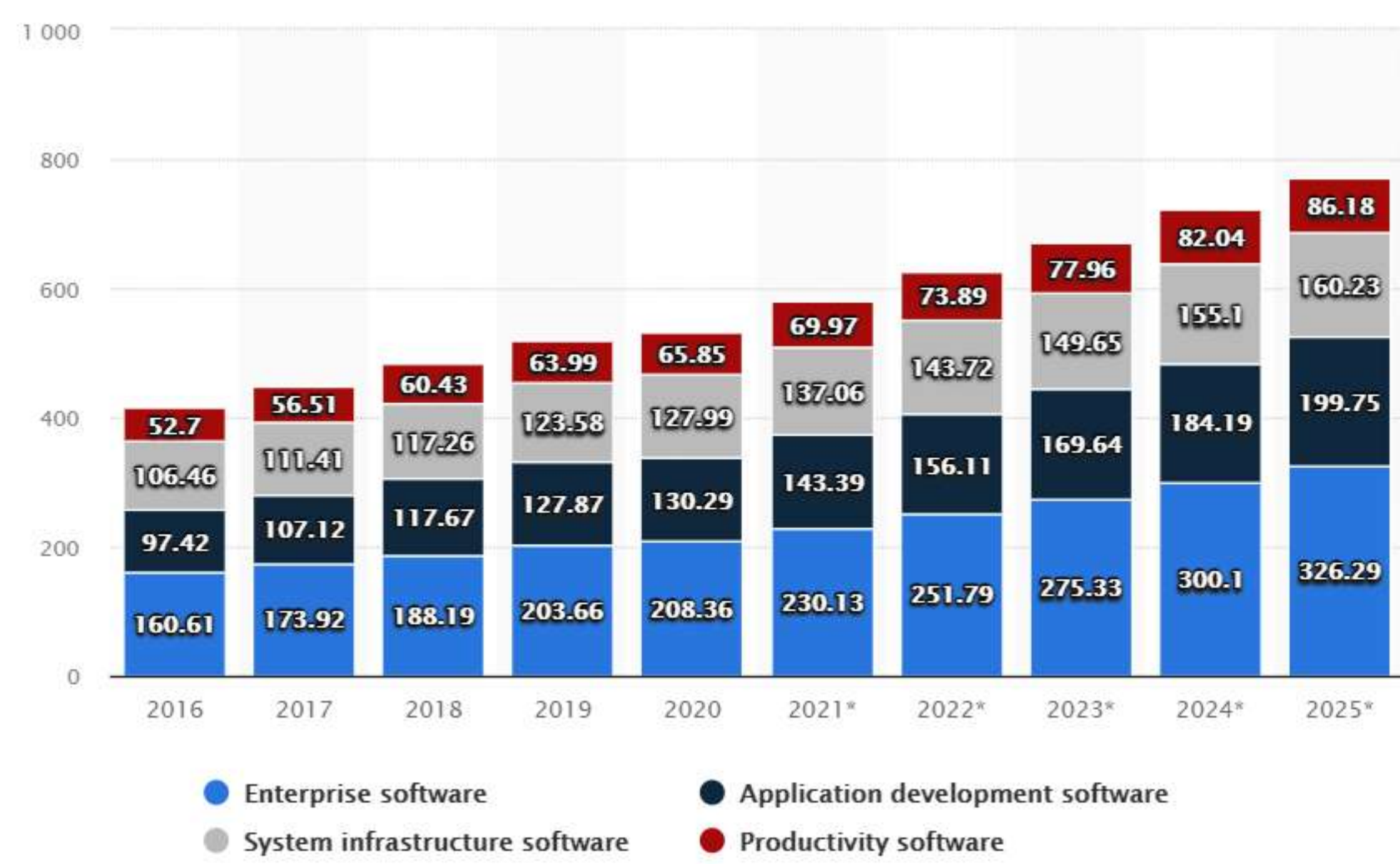
In 2018, the software market revenue was registered at \$456.1 billion and now expected to reach \$507.2 billion in 2021. Moreover, the COVID outbreak raised the situation of economic downturn and allowed companies to keep a small budget for software solutions, resulting in market contraction in 2020. However, the pandemic teaches companies to address the urgency of digital transformation and make it part of success.

How vast is the digital world ecosystem?

Software Development & Developers Market

The rapid advancement of technology makes this digital world more buzzing and more dynamic. And, software development acts as a fuel that drives our IT services at high speed. Most of the software market is covered by enterprise software that faces a decline in 2020 due to COVID, but soon it resumes its growth in 2021 as per Statista Forecast.

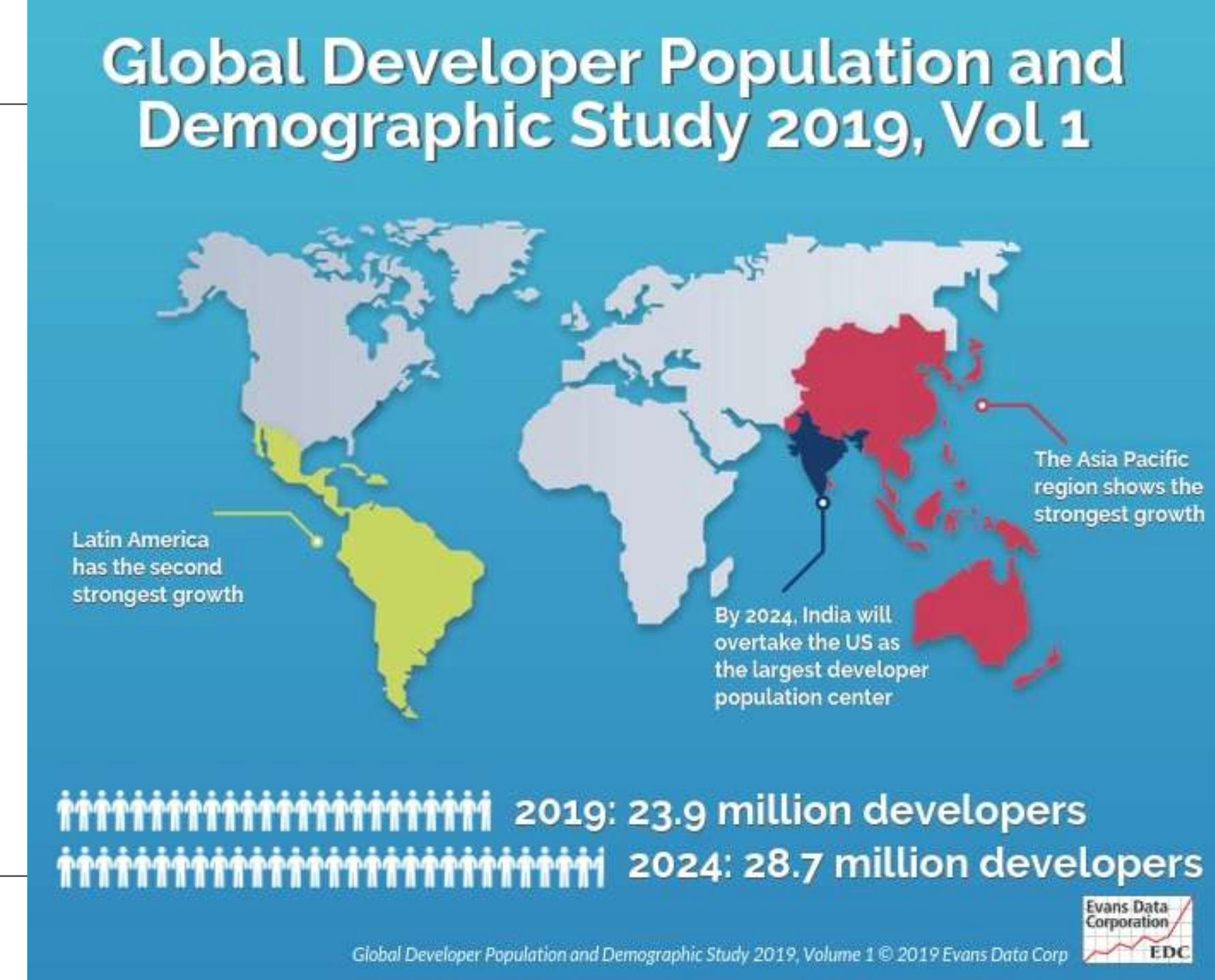




As always, the outline of software needs utmost attention to the end-user experience. However, digitalization compels industries to step forward to adopt cloud application services or SaaS (software as a service) to amplify user engagement. Although, the market still opens for other forms of software.

Year	Number of Software Developers
2018	23.9 million
2019	26.4 million
2023	27.7 million
2024	28.7 million
2030	45 million

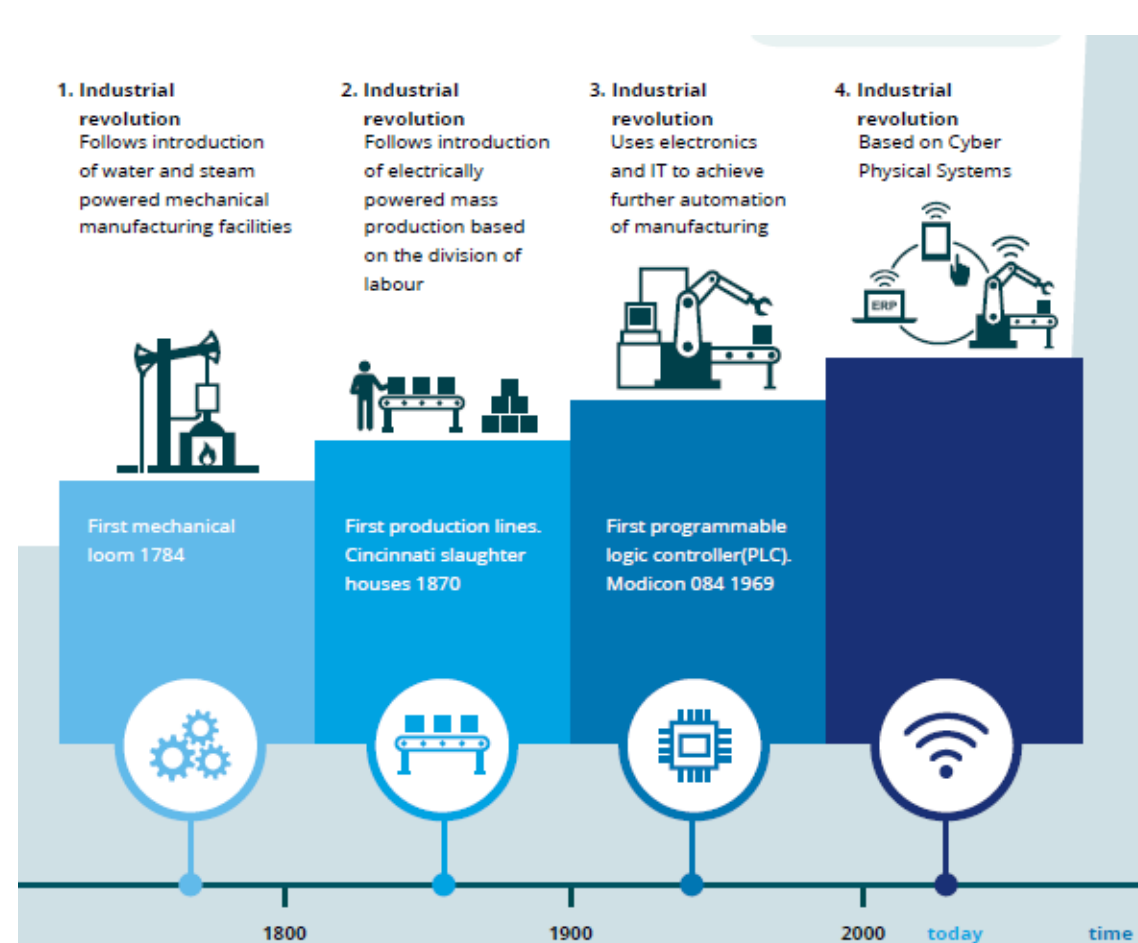
The calculation of Evans Data Corporation estimates 26.4 million software developers in the world in 2019 and is expected to touch 28.7 million in 2024. Quite interesting, India will overtake the U.S. as the largest developer population center in 2024.



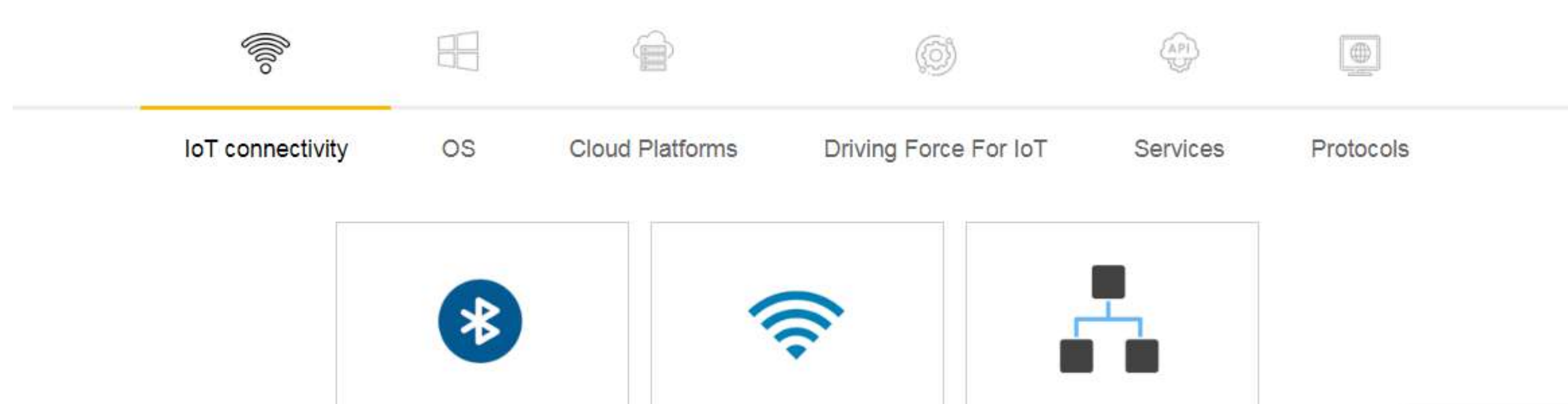
According to the Statista Technology Market Outlook, the central part of worldwide software revenue comes from Enterprise software, which is calculated as over 200 billion U.S. dollars in 2020 and is expected to reach good heights in upcoming years.



Industrial revolutions in a digitally-enabled ecosystem



CyberSecurity and cloud-based applications are some of the significant aspects of the industry's rapid development. Now, it is termed Industry 4.0 and brings drastic changes into our lives, from mechanical manufacturing facilities to cyber-physical systems.

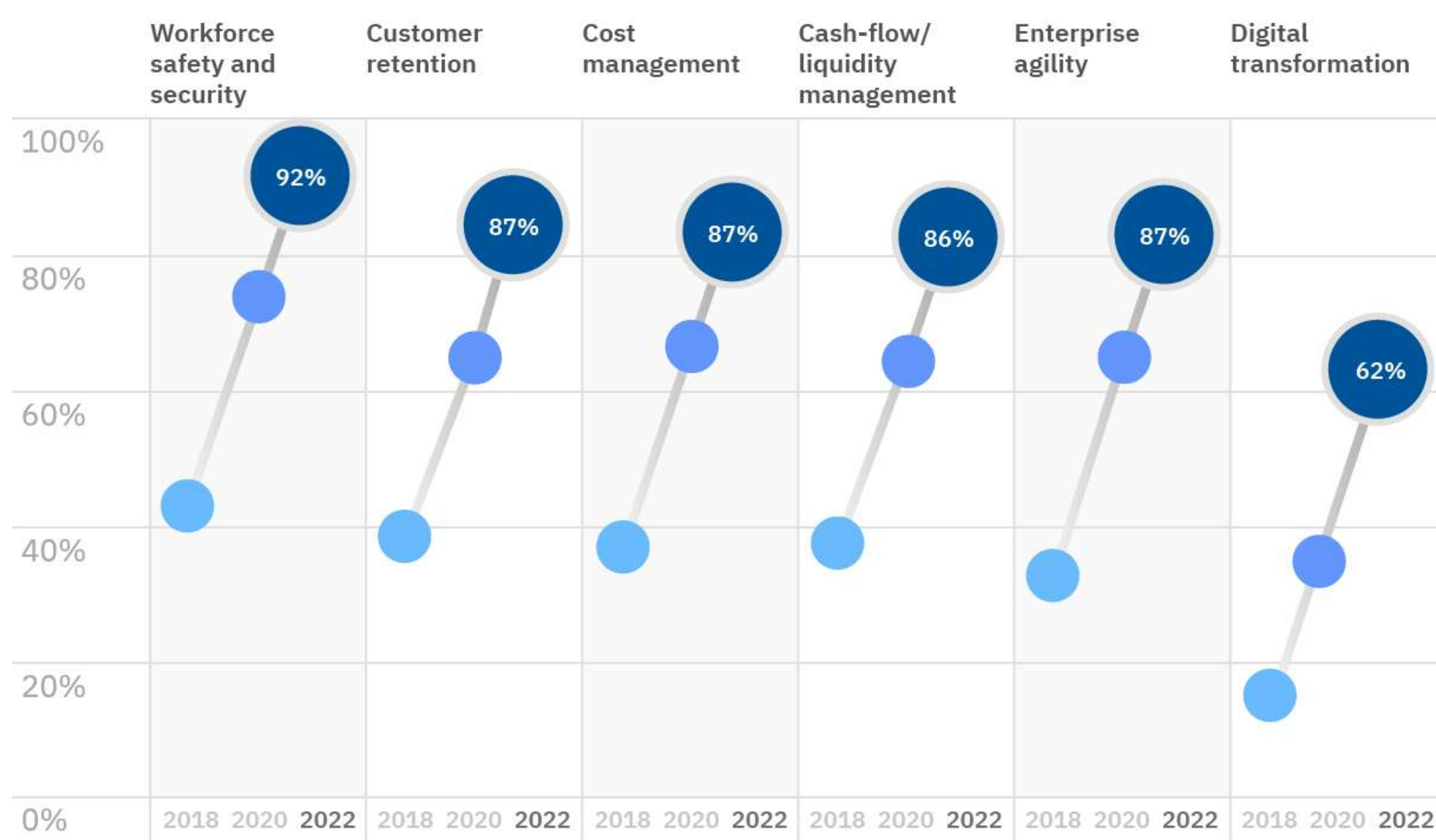


ValueCoders' software outsourcing services are dedicatedly working to make a more secure digital enterprise. We focus on catering smart connected solutions through IoT (internet of things) and advanced app development.

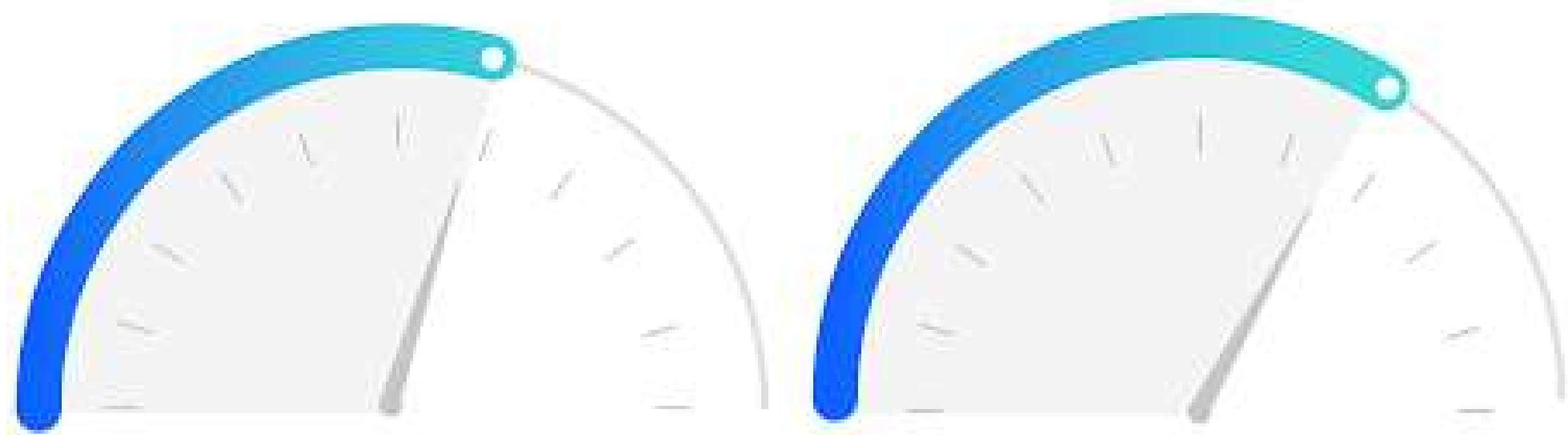
Future Industry Digital Ecosystems	Digital Technologies Disrupting/Providing Growth Opportunities in the Industry	Converging Industries
Connected Health Care	IoT, Analytics, Cloud, Wearables	Healthcare, Fitness, Pharmaceutical, Technology, Apparel, Telecom
Connected Automobile	IoT, Cloud, Big Data, Cognitive Automation	Automobiles, Technology, Energy and Utilities, Telecom, Insurance
Smart Home	IoT, Analytics, Cloud, Cognitive Automation	Technology, Consumer Electronic Goods, Energy and Utilities, Telecom, Healthcare

More connectivity to cyber amplifies the significance of data security. In the case of data handling, telecom operators are one of the few entities to focus on. Also, data is a fundamental element of B2B2C models to sustain the growth of the telecom industry in India. While advancing the digital framework in the telecom ecosystem, one has to include key players such as mobile apps (WhatsApp, Skype), Internet Service Provider (ISP), App developers, Communications Service Providers (CSP), and Device manufacturers. Here, more engagement raises the concerns of data privacy that needed to be expanded beyond the I.T. Act.

Software requirements after COVID pandemic



COVID 19 pandemic unfolded the urgency of digital transformation to meet software requirements. Companies need to address the new face of this information world. Recent research of IBM Institute for Business Values demonstrates the shifting interest in digital transformation from other core elements such as cost management, customer retention, etc.



59%
Accelerated digital transformation

66%
Completed initiatives that previously encountered resistance

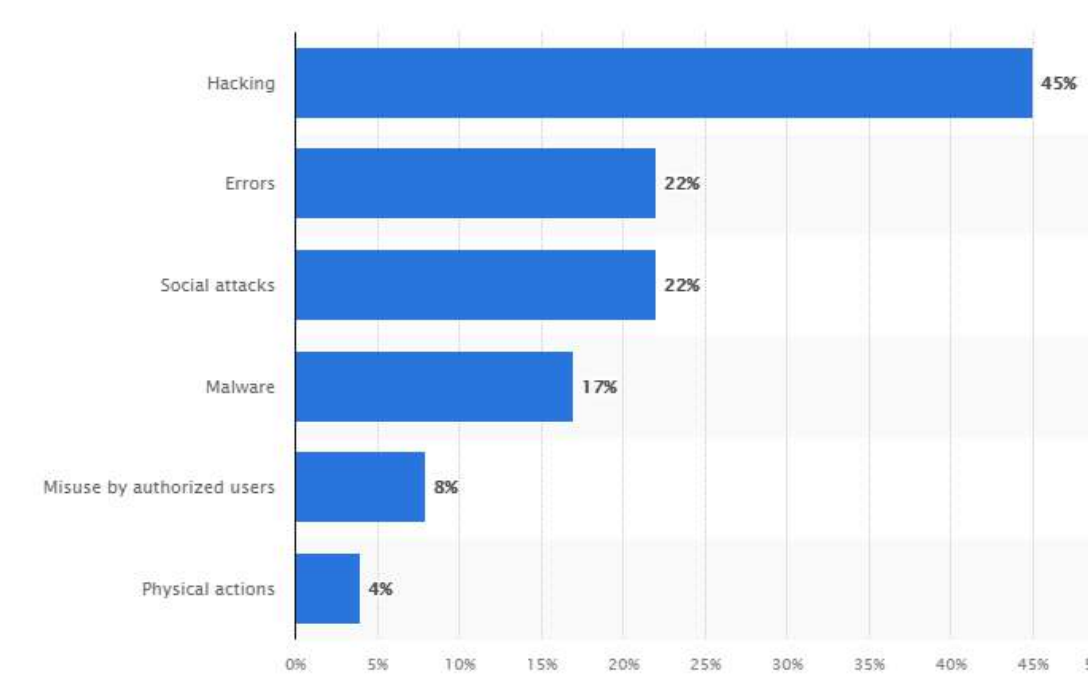
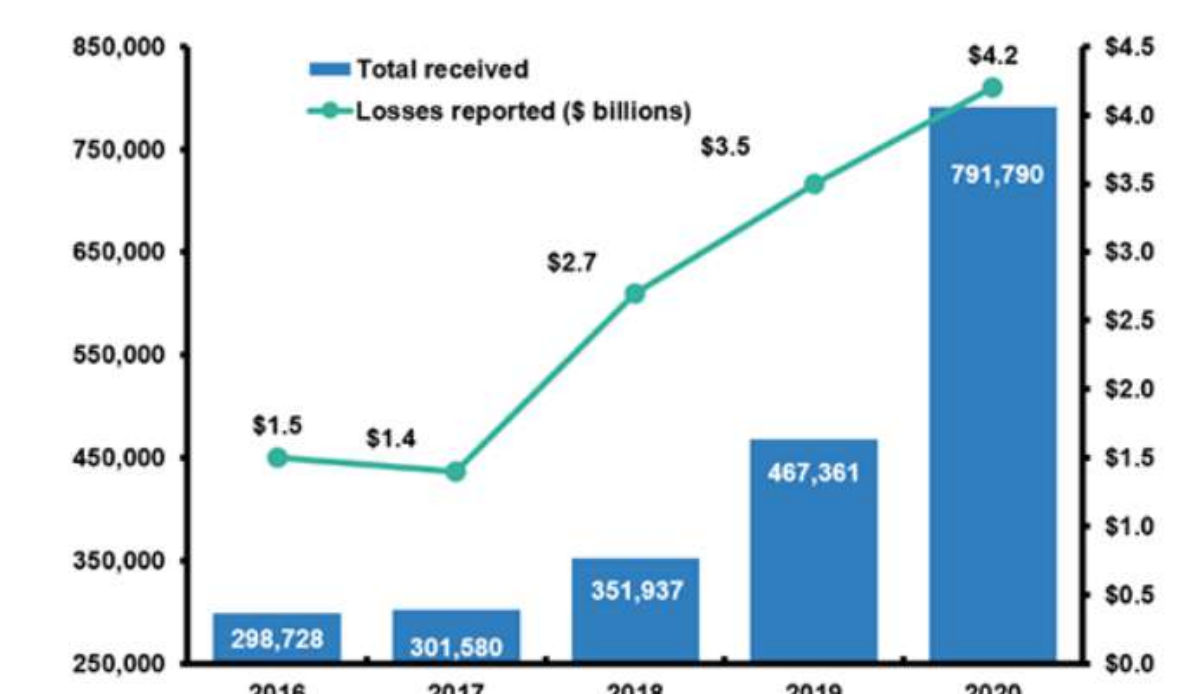
59% of companies accelerated digital transformation, and the remaining 66% have finished the previously encountered resistance. Organizations are reshaping their strategies and investing in the latest technologies such as IoT, blockchain, etc., as an active recovery of a pandemic. This paradigm shifts the attention of companies into the following matters:

- Software product engineering emerges as a new software development model to build customer-facing and market-oriented software.
- COVID-19 High-Performance Computing (HPC) Consortium is joined by top companies Amazon, Google, and Microsoft for computational research programs.
- A business partnership is a new success strategy to excel the business ventures and expansions.
- More attention is shifted to hybrid cloud and taking business functions to the cloud.

Security thefts in Software Engineering

Cybercrime Data analysis

The rapid advancement of technology makes this digital world more buzzing and more dynamic. And, software development acts as a fuel that drives our IT services at high speed. Most of the software market is covered by enterprise software that faces a decline in 2020 due to COVID, but soon it resumes its growth in 2021 as per Statista Forecast.



On average, the cost of a data breach is about 3.86 million U.S. dollars in 2019, and the prominent victim is the healthcare sector with 7.13 million dollars. A complete analysis of statista talks about financial repercussions in business based on region and size of companies.

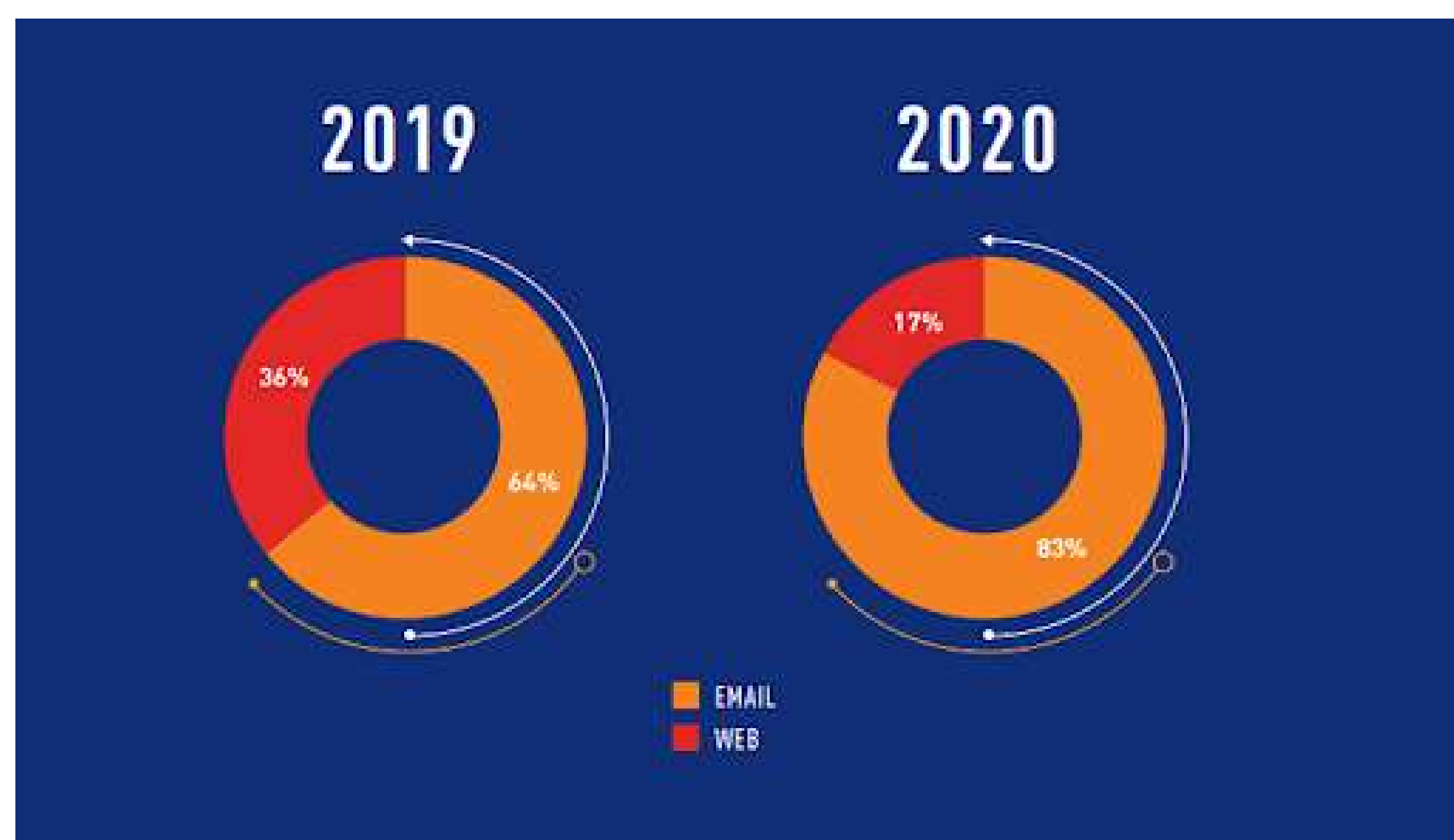


Every type of cybercrime leads us to data breaching, and hacking is one of the most common criminal activities on the internet. Hackers exploit a weakness in online communication or digital networks, computer systems and spread malware or gain unauthorized access to data for pursuing their criminal activities. All actions uplift the urgency of a robust defense system to stop cyber attacks.

While discussing data breaching, social media also is a massive center of attraction. However, many users are skeptical about the data being used. Giant social media platform Facebook received 61,262 law enforcement agency requests from the U.S. and 40,300 data requests from India to know about user information. Indirectly, it raises questions over the maximum use of social media.

Web applications vulnerabilities and threats

Misconfiguration in web application code allows hackers to get control over your website. That's why the security of software development raises concerns to address web applications vulnerabilities and threats. The US government's National Vulnerability Database (NVD) shares the case studies of cybercrimes of prominent organizations.



According to Tenable's 2020 Threat Landscape Retrospective Report, about 22 billion data were exposed in data breaches globally in 2020. For more insights on ransom attacks, go through the pick points of Check Point Cyber Security Report 2021

- Increment of 20% in email-based attacks from 2019 to 2020 as compared to web attack vectors.
- In 2019 and 2020, Emotet was the most heavily distributed malware family. It is a botnet responsible for the distribution of Trickbot, Qbot, and more, in some cases resulting in a ransomware attack.
- XMRig is the most attacked cryptominer, whereas Lucifer is a self-propagating, multi-platform malware targeting Linux, IoT devices, and Windows web servers.
- Hiddad or 'Hidden Ad' tops the chart of mobile malware global analysis. Through this malware, attackers can easily fetch the details from victims' mobile by displaying ads. During COVID, the malware disguised itself as a coronavirus information app for Arab speakers.
- In 2020, a team of developers took 280 days to identify a cyber breach that led to the loss of nearly \$4 million.

How to approach secure software development?

Secure Development Lifecycle (SDL)

Cyberattacks and enhanced data security directs companies to think about secure software development. ValueCoders is a software outsourcing company that continuously addresses defects to make secure software and reduce vulnerabilities. Divide software development lifecycle into different segments starting from requirements and move to other steps, designing, implementation, and testing.

The Software Engineering Institute developed the Team Software Process (TSP), allowing software developers and developer teams to create software under a definite process. This process wants companies to focus on:

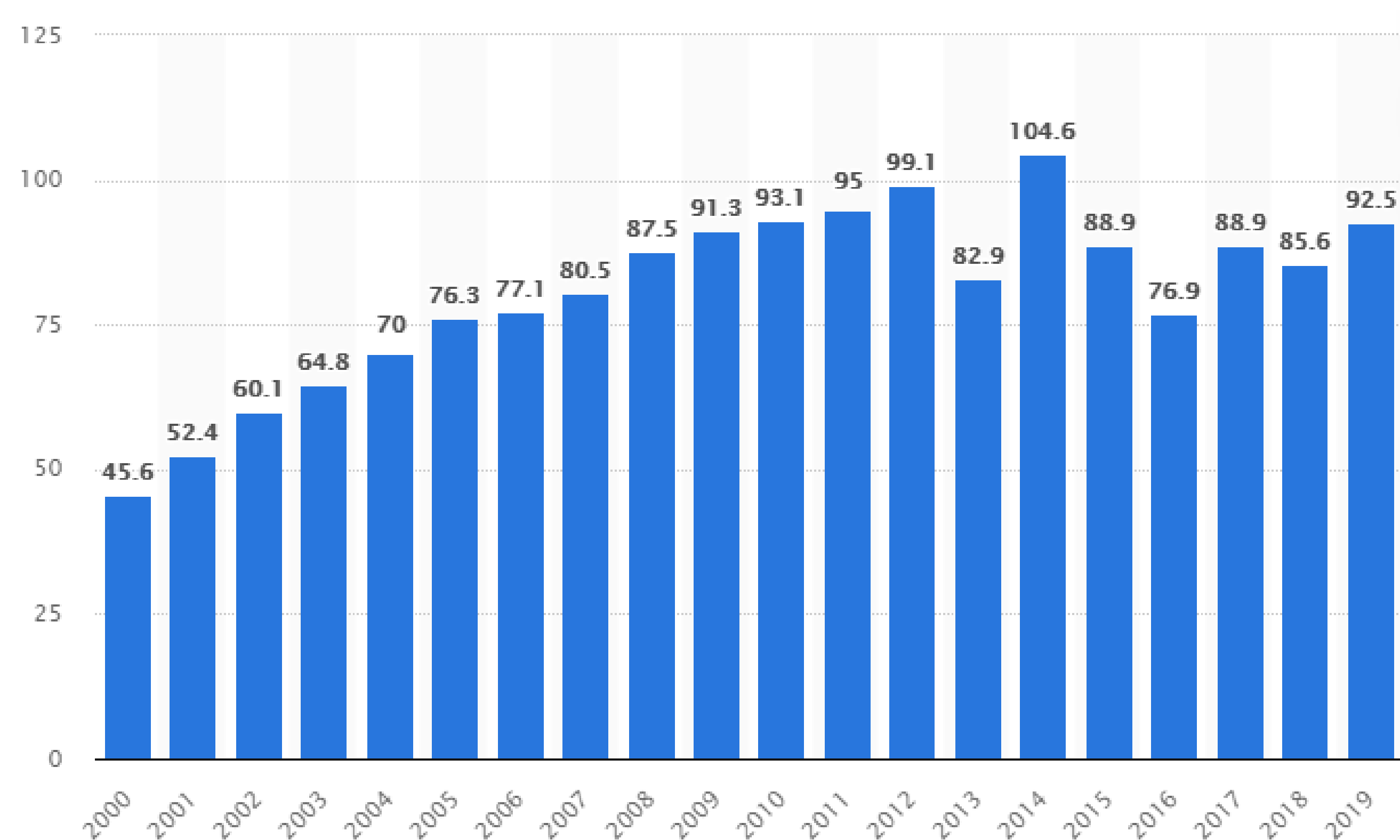
- Use common sense software engineering practices
- Tackle defects throughout the software product development lifecycle
- Use proper measurement to control the process
- Track the process and address defect prevention as well as removal
- Apply predictive measures for remaining defects

Another significant example demonstrated by Microsoft Security Development Lifecycle (SDL) practices. SDL practices support security assurance and compliance requirements and also reduce the severity of vulnerabilities in software development.

As per Microsoft, software developers are suggested to follow various practices:

1. Providing training
2. Define security requirements
3. Define metrics and compliance reporting
4. Perform threat modeling
5. Establish Design requirements
6. Define & use cryptography
7. Use third-party components to manage the security-risk
8. Use approved tools
9. Perform Static Analysis Security Testing (SAST)
10. Perform Dynamic Analysis Security Testing (DAST)
11. Perform Penetration Testing
12. Establish a Standard Incident Response Process

Offshore Software Development Services



Maintaining software security favors offshore software development services for enhanced data security. Costing and quality services are the main focus areas of IT outsourcing services. The market for outsourcing services is enormous. In 2019, the global outsourcing market registered as 92.5 billion U.S. dollars and was expected to reach over USD 98 billion by 2025. It's gaining popularity because of offering the latest technologies such as cloud computing, blockchain technology and expanding the digital transformation.

About us

ValueCoders is a top software outsourcing company in India and is making an effort to provide an enhanced digital experience via secure software development. After stepping the foundation stone in the technology era in 2004, the company successfully maintained 97% client retention and has delivered 4200+ projects so far.

With business domain knowledge, proven methodologies, and technology expertise of 450+ skilled software professionals, ValueCoders delivers IT outsourcing services worldwide. Build a dedicated development team with the right technology stack at

<https://www.valuecoders.com/>