scalefocus

2020 CyberSecurity Trends on Focus

The numbers are in ...

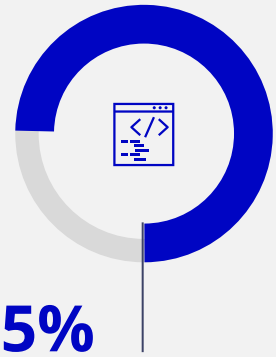
Without a doubt, the past year has proven to be a whirlwind for societies worldwide. Businesses have been trying to stay afloat and find opportunities in the crisis, while protecting their data and networks from malicious attacks. We've gathered some key statistics and findings from leading security reports to give you the big picture on the current cybersecurity environment.

99%

of **vulnerabilities** exploited are known by **security & IT professionals.**[1]

280 days:

average **time** to **discover** and **thwart threats.**[3]



75%

of **open source** software include **known vulnerabilities.**[3]

3.86 mil.

average total cost of **data breaches.**[3]

Healthcare is the **highest costing industry to secure.**

1. Earl Perkins, MVP Adaptive Resilience, Trust and Risk Management, Gartner
2. Synopsis: 2020 Open Source Security & Risk Analysis
3. IBM Security: Cost of a Data Breach 2020

Gaining Visibility on Known Vulnerabilities

An astonishing 64% of employees have confessed to not being fully aware of their company's web applications or endpoints, while 68% of security professions admit to performing a mediocre level of device monitoring.

As companies expand, so does their digital output and potential for data breaches. Small organizations with 11-100 staff, carry a 4% medium-critical threat risk; 101-1000 staffed companies hold a 35% risk; 1001-10000

staffed hold 40.5% risk; while companies with over 10000 staff hold a slightly lower 30% risk. The company size also impacts the time to contain a vulnerability, with the lack of resources in smaller companies resulting in 56-73 days compared to 61 days in companies with over 1000 staff.

And while over 8 billion breaches were recorded last, year, the oldest vulnerability discovered was twenty years old, from 1999: CVE-1999-0517. Although its occurrence rate is 1.75% its CVSS severity score remains high at 7.5. In 2020, 27% of company assets worldwide have a score of 7.0 or higher. (2020 Edgescan Vulnerability Statistics Report)

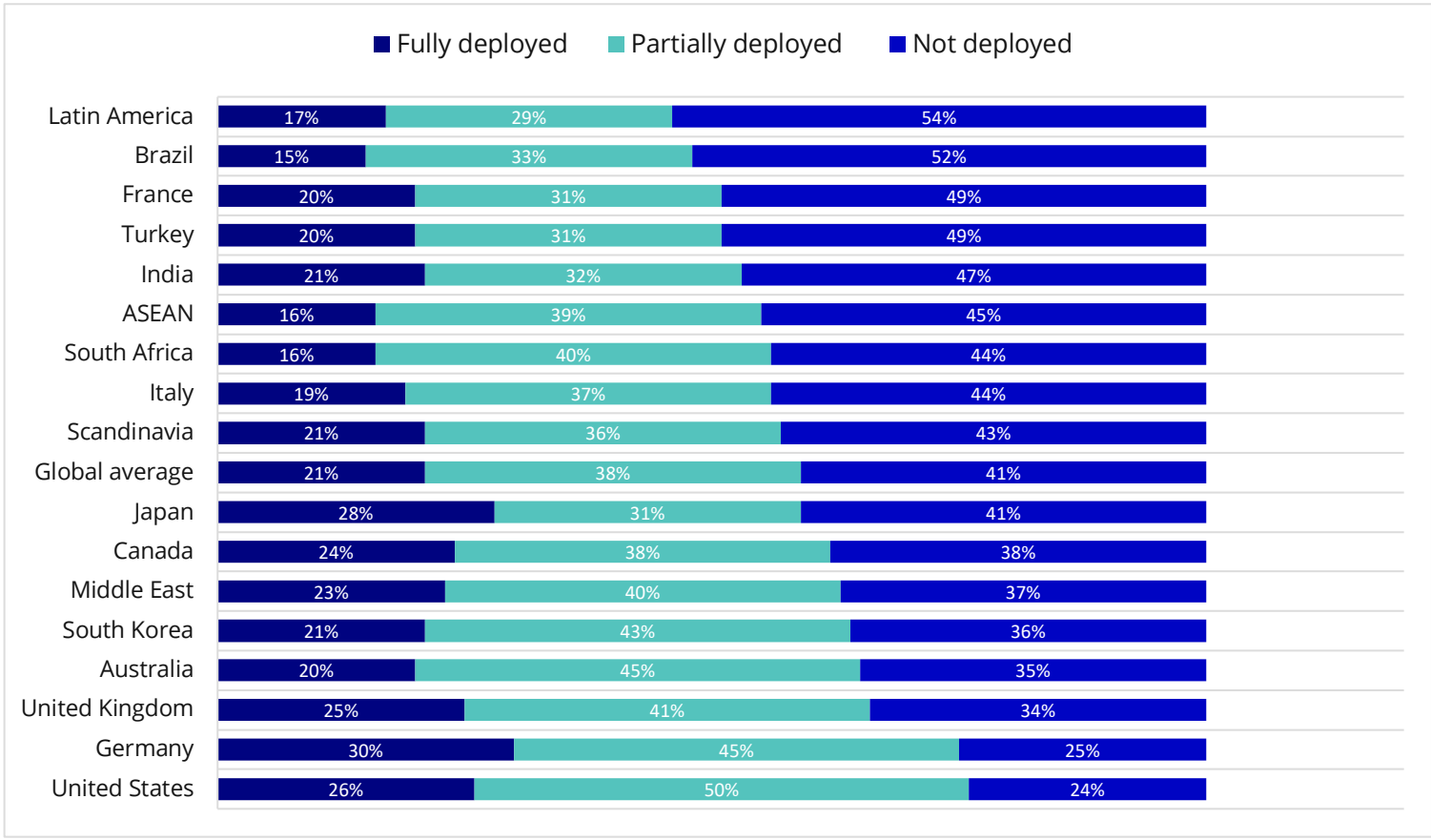
Optimizing Cost and Time

Organizations save an average of $1.12 million if they manage to contain a breach in less than 200 days. Comparing industries, the financial sector has the shortest data breach lifecycle, on average taking 233 days to identify and contain, while healthcare comes in last with 329 days.

When fully deployed, security automation has managed to cut the data breach lifecycle to 175 days, compared to 275 when it is partially deployed and 308 when there is none. U.S.A, Germany and the United Kingdom are the top three nations that have introduced automation as part of their cybersecurity strategy. (IBM Security: Cost of a Data Breach Report 2020)

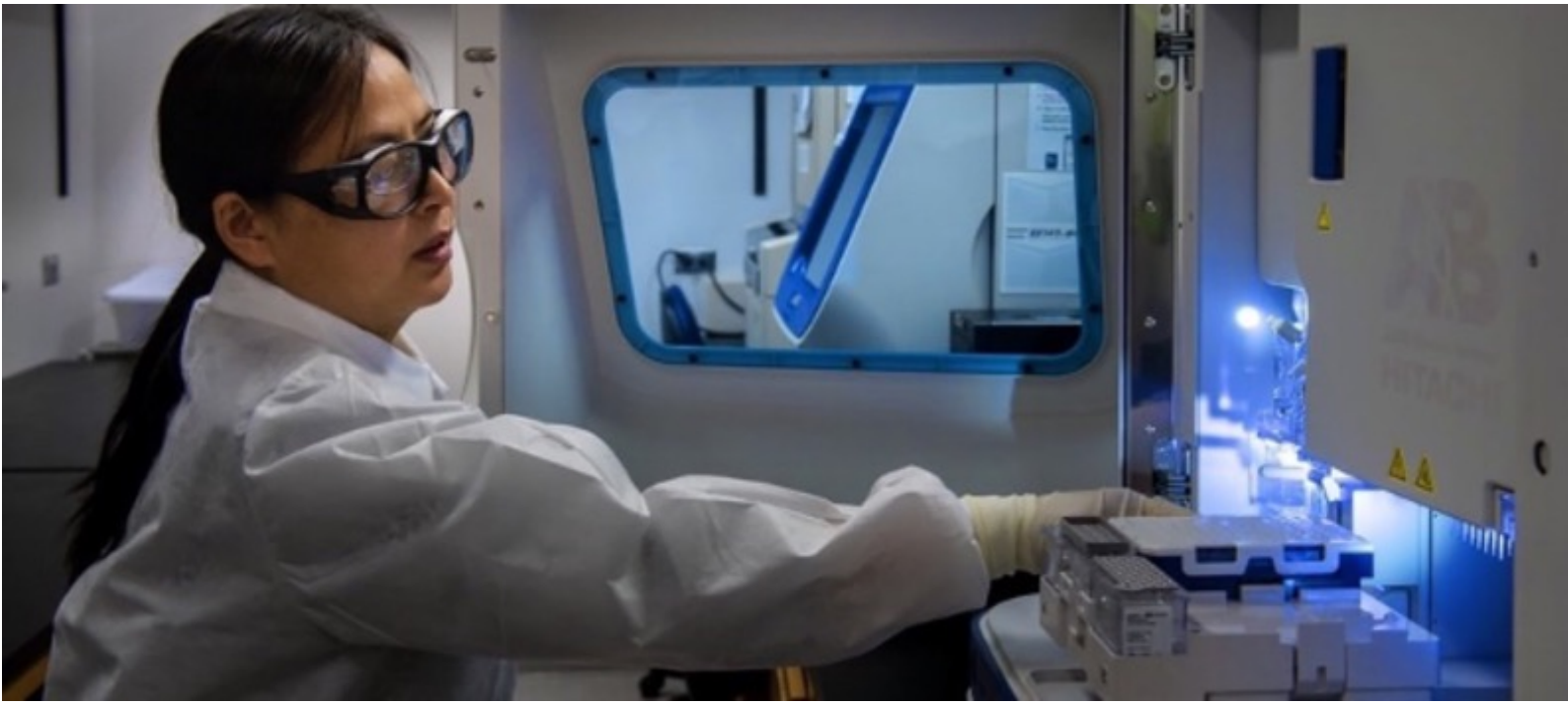
Average security automation deployment by country

Percentage of organizations in three automation levels:



Keeping Focus During a Crisis

The negative effects businesses have experienced during the Covid-19 pandemic are unprecedented. Introducing remote work has led to a slower response time to identify and contain data breaches.



The immediate need for personal protective equipment (PPE) has also pushed organizations to stock up supplies from potentially malicious sites. As telehealth offerings including treatments and lab results are surging, so is patient online data with loopholes for cybercriminals to enter through. Now more than ever, businesses must shift their attention towards ensuring all-around data protection and network security.

2000%

increase in **malicious Zoom-titled** files. (Webroot)

6 billion

"Covid-19" search results with 90% of newly created domains **being scams**. (ZDNet)

>67%

breaches coming from **phishing and credential theft**. (Verizon)

40%

rise in **unsecured remote** desktop machines.(Webroot)

Your Next Steps

- **Create a cybersecurity strategy** that you will closely follow.
- **Ensure clear asset visibility** throughout your entire organization.
- **Stick to patch management** best practices.
- **Enforce regular security trainings** and promote cyber hygiene
- **Seek expert help** from a security provider after doing your research.

Strengthen and protect your critical data by partnering with trusted security professionals. Explore how CyberSec Risk Manager can close your vulnerability gaps and lead you to make smarter business decisions. Reach out to begin your exciting journey with Scalefocus.

CONTACT US

scalefocus.com

csrm@scalefocus.com