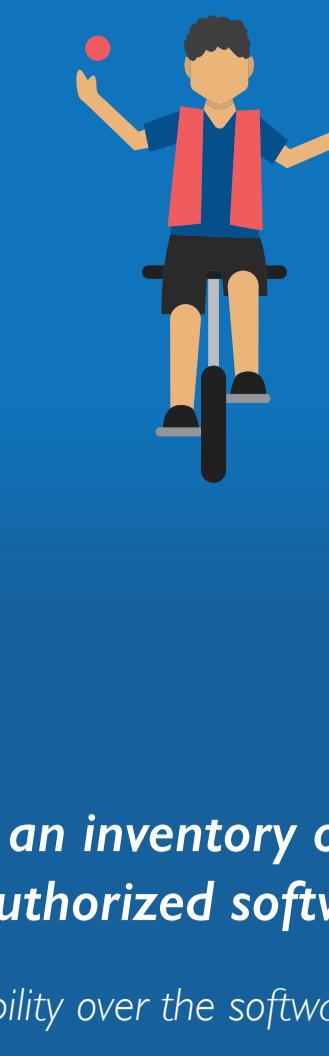


Ten security controls for effective cybersecurity



Keeping an inventory of authorized and unauthorized hardware

Maintaining and securing remote network devices—whether they're laptops or mobile devices—can be challenging but should never be neglected, as each device is another opportunity for an attacker to sneak in. Encryption and endpoint management can help.

1

Keeping an inventory of authorized and unauthorized software

Having visibility over the software in your network can help you identify and remove prohibited software as well as the risk of unknown software exploitations.

2

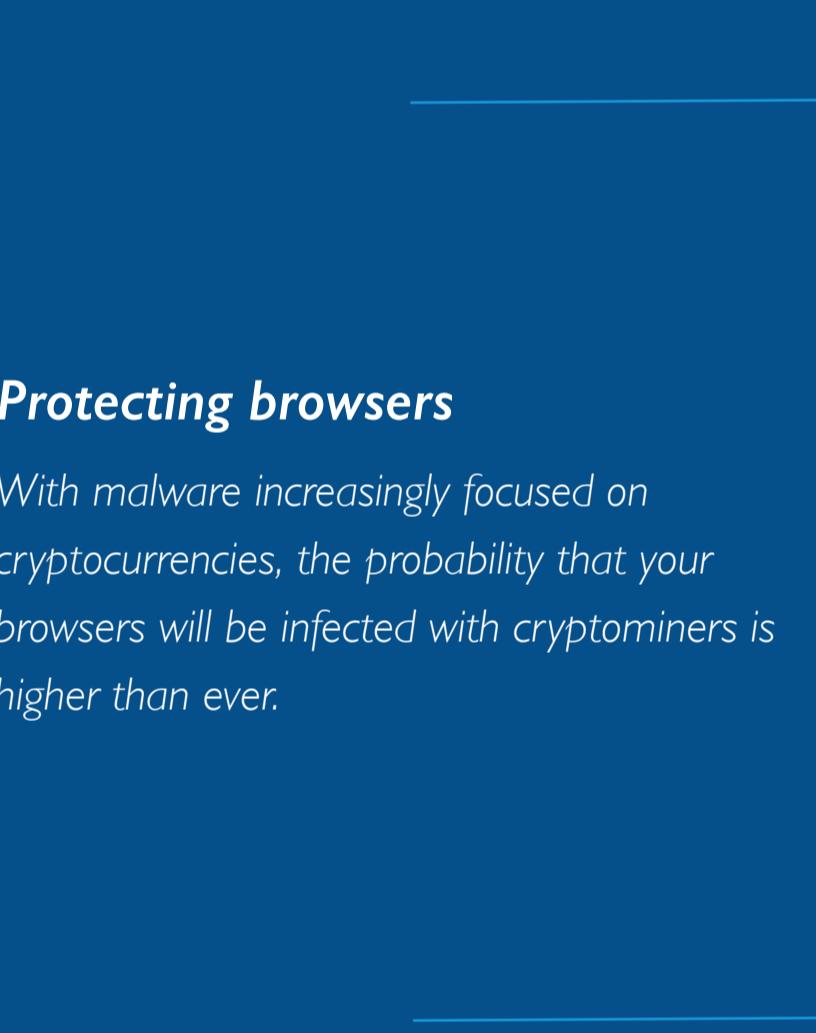
- 2016 brought us the **Mirai botnet**.
- 2017 brought us **Brickerbot malware** and the **CloudPet breach**.
- 2018 will bring us more focused and **aggressive attacks** than before.

3

Securing hardware and software configurations

Customized configurations for hardware and software can help mitigate both hardware and software-specific attacks.

Do remember there are **230,000 new malware** identified every day



Average cost of a data breach will exceed **\$150 million** by 2020.

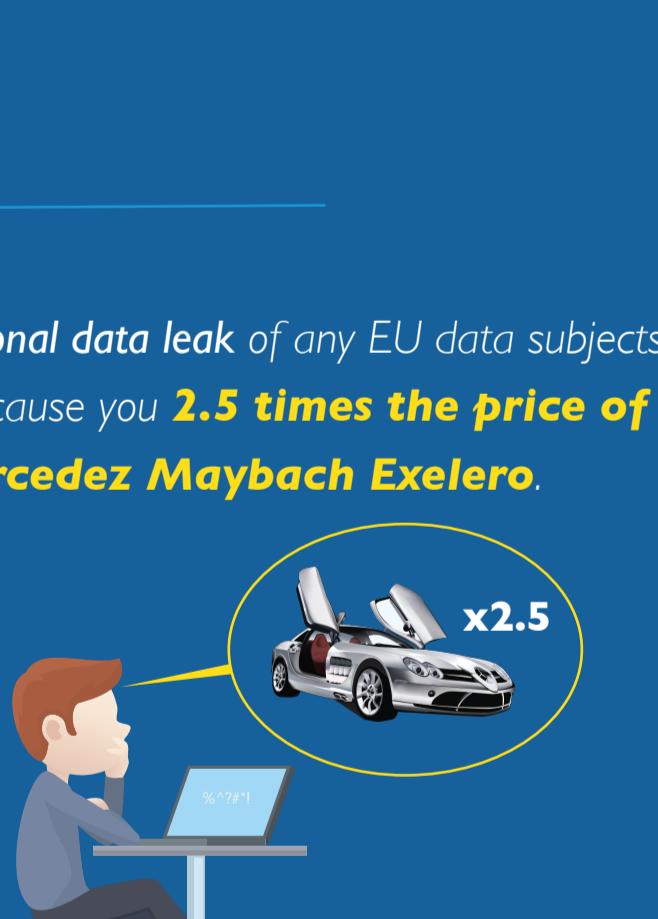
Protecting browsers

With malware increasingly focused on cryptocurrencies, the probability that your browsers will be infected with cryptominers is higher than ever.

Since 2013 there are **3,809,448** records stolen from breaches every day, **158,727** per hour, **2,645** per minute and **44** every second.

4

A cyber attack happens every **39 seconds**, victimizing **1 in 3 Americans**.



Through 2020, **99%** of exploits will continue to be ones known by security and IT professionals for at least one year.

5

Ensuring access control and administrative privileges are accurate and in constant use

With the GDPR and DPB (data protection laws) already in effect this year, comprehensive data security is no longer just good business sense, it's also mandatory.

6

Cryptjacking is set to take down enterprise devices for mining in 2018, as the **cryptocurrency buzz escalates**.



64% of companies experienced web-based attacks. **62%** companies have faced phishing & social engineering attacks. **93%** of phishing emails are now ransomware.

7

In 2018, cybercriminals will target and exploit more security software

Eternalblue – a port vulnerability that affected more than **300,000** computers worldwide.



65% companies have over **500 users** with passwords that never expire

8

Personal data leak of any EU data subjects, can cause you **2.5 times the price of Mercedes Maybach Exelero**.



Source: nvd.nist.gov (19th Sep 2018)

9

Monitoring and controlling accounts

Often, expired user accounts are not removed from directories, meaning they leave a gap in a company's security. Likewise, passwords that never expire increase that account's vulnerability over time. Stay on top of security gaps by monitoring account activity and controlling password policies.



Achieve and sustain these ten security controls using **Desktop Central**.

[Download Now](#)

Disclaimer: The above information is a collective report of various statistics available on the web.