ENERGY LOGSERVER

Big Data in 2022

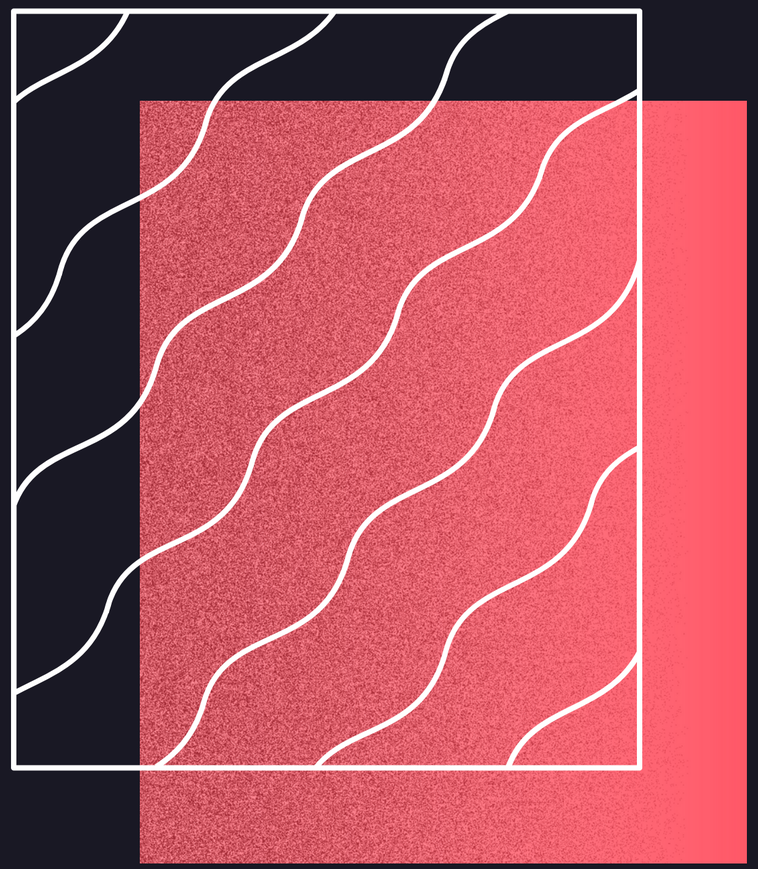
Report: What the future holds for us?

ANOTHER YEAR IN A PANDEMIC WORLD

2021

WHAT WE LEARNED?

Accelerated by the global pandemic that pushed digital transformation to go much further and much faster, companies in 2021 ended up having complex environments that continuously generate new data. Such "tsunami" of unanalysed information can certainly drown the IT environments, therefore, owning an efficient data management system has slowly turned into a necessity for every company.



THE DATA BECAME TOO BIG AND COMPLEX FOR TRADITIONAL SOC TEAMS TO MANAGE

It’s not cheap to purchase or subscribe to data management service, and implement it afterward, but it’s still far more efficient than a team of 20 data analysts. Besides, the talent and resources required to maintain such amount of data in a proper way, turned out to be even more costly, and yet less successful than a dedicated machine.

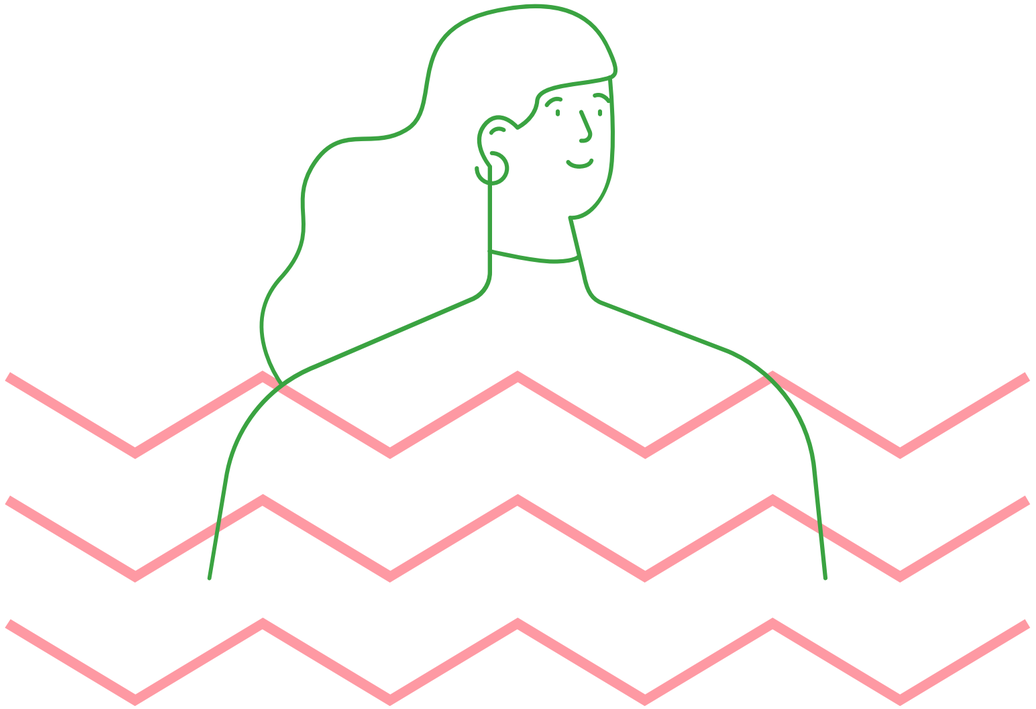
Ultimately, a machine is much faster than a human—or even a group of humans, and the new technologies are having way smaller chances of misunderstanding the language on which the system is trying to warn us. Eventually, this is leading to one of the biggest threats that the companies were dealing with in 2021.

DATA BREACHES AND CYBER-ATTACKS IN 2021

We live in a times when the cybercrime is the greatest threat to every company in the world. Unlike large corporations who have the money and resources to pay for cybersecurity and upgrade their network match the latest hacker tricks, small businesses do not have that same “luxury”, and hackers know it. Therefore, around half of the attacks target the smaller business.

Nevertheless, with evolving technology came evolving hackers, and even the richest companies aren’t immune to the cyberthreats. This year we could hear about the data breaches in some of the richest companies in the world: Colonial Pipeline, Facebook, Instagram, LinkedIn, Amazon, e-Bay, and many others...

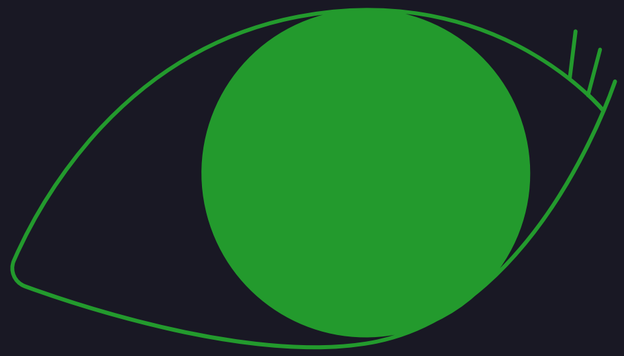
According to Identity Theft Resource Center (ITRC) research, the number of data breaches through September 30, 2021, has exceeded the total number of events in full-year 2020 by 17 percent (1,291 breaches in 2021 compared to 1,108 breaches in 2020).



GETTING USED TO THE NEW WORKING STANDARDS AND THE STRUGGLES OF WORKING FROM HOME

A remote workforce comes with countless dangers, from employees relying on their home networks – to using their own personal devices – to complete work tasks. Moreover, without the security protections that office systems afford us, we became far more vulnerable to cyber-attacks. According to the "Velocity Smart Technology Market Research Report 2021", 70% of remote workers said they had experienced IT problems during the pandemic, and 54% had to wait up to three hours for the issue to be resolved.

Yet, for better or worse, remote working is here to stay, with the benefits and the comfort too attractive to resist.



HERE ARE SOME FORCASTS FOR 2022

THE WHOLE IDEA OF AN OFFICE SPACE NEEDS A MAKEOVER

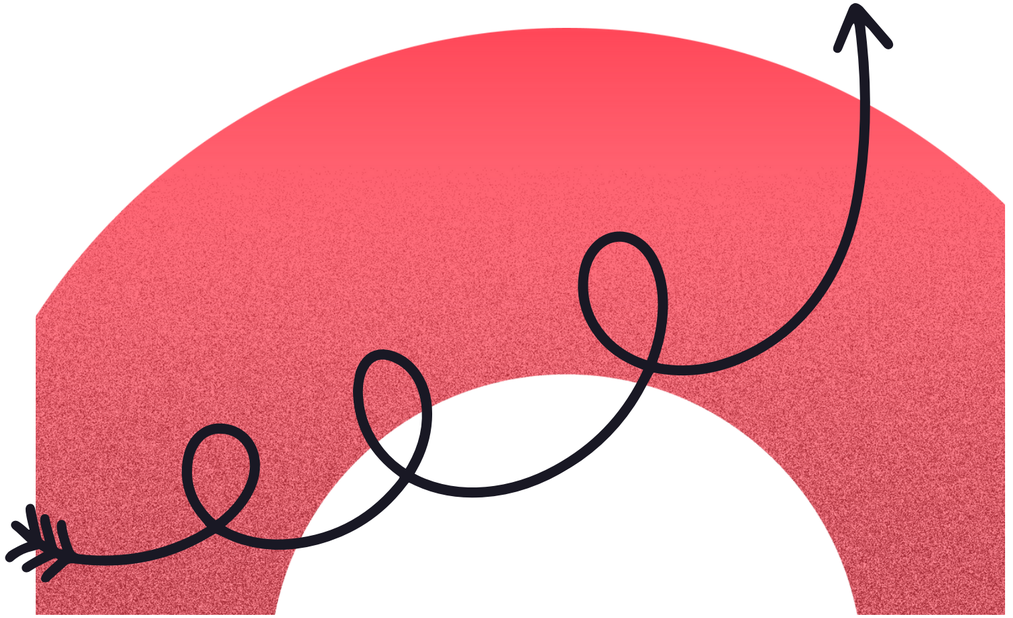
What we definitely can’t see on the 2022 roadmap, is the day when most people will work most days in an office. Be prepared for a hybrid workforce of office regulars, full-time remote workers, and a substantial group that tries to find a balance between these two alternatives.

In general, we could notice that the whole idea of the office was changing in the past two years, and this process of transitioning will start getting more concrete shape in 2022. We no longer can see the office as the primary workplace, but more of an integration point, a place where teams meet to bond, find inspiration, and maybe find a quiet corner to get some solo work done.

CYBER SECURITY TRENDS IN 2022

As result of the changes in the work environments caused by Covid 19, the explosion of data available to a company has made the use of artificial intelligence (AI) and machine learning (ML) a critical competitive advantage. As organisations look to improve their security postures in response to the evolving threat scenery, for example, they may look for security tools using Artificial Intelligence to perform tasks.

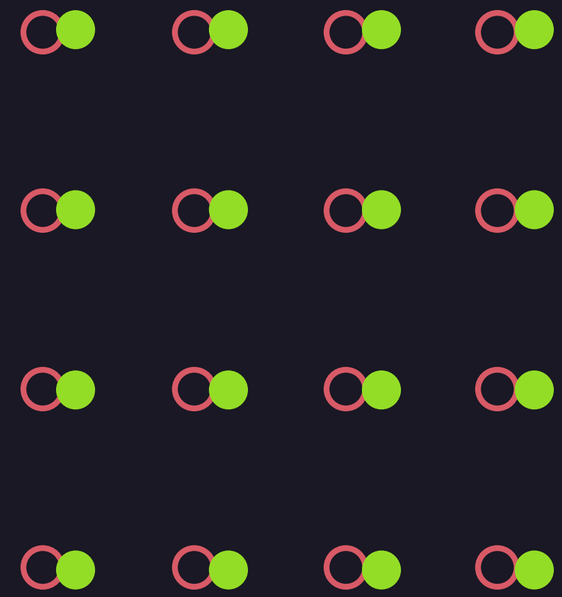
One of the biggest data trends is becoming the usage of big data analytics to power AI and ML automation, both for internal operations, and for consumer-facing needs. Organizations of all sizes will be more actively turning to smart data fabrics as it provides the capabilities needed to discover, connect, integrate, manage, utilize, and store data assets to enable the business to meet its goals faster and with less complexity than previous approaches.



Cybersecurity skills shortage will drive to more orchestration and automation. While there has already been an ongoing lack of labour in IT/IoT security, the shortage in OT security is far more drastic. Very few professionals and college programs focus on operational technology cybersecurity, and it will take many years to fix this problem. Enterprises will have no choice but to focus on more automation to provide better data understanding and make more conscious decisions putting a pin on visualization and analytics of all collected data.

Big Data management and incident response currently have enough solutions targeted at them. The greatest challenge in 2022 will be to switch from technology to efficient operating the incidence response, SOC setups. With so many advanced cybersecurity solutions, and so few people to manage them, in the past two years enterprises struggled to incorporate global-wide cybersecurity. As a result, it’s expected that in 2022 the enterprises will try to move away from siloed, stand-alone cybersecurity solutions to either platform-based software or tools that can provide integration with many other tools.

CYBER SECURITY TRENDS IN 2022



HOW TO MAXIMISE THE VALUE YOU GET FROM YOUR SYSTEMS DATA IN 2022?

Huge part in the increment of the big data over the last few years has come in the form of consumer data that is constantly connected to consumers while they use their personal technology (such as streaming devices, IoT devices, and social media). AI and ML solutions are already futuristic on their own, but the automations and workflow shortcuts that they enable are the main business game changers.

The Big data analysing technology is constantly improving, and in 2022 will help to more and more businesses to become better supplied, make informed decisions, and develop effective strategies to improve their market positions.

At the end, our advice for successful business management in 2022 is monitor the way your sensitive information is used, try to turn it into a business advantage, check for vulnerabilities in your systems, adapt to the latest data protection requirements and respond promptly when a cyber incident occurs.

Following this and all the previously mentioned security threats and trends, 2022 will be another year in witch Energy Logserver will continue it's efforts to evolve and boost the existing technology in a way that will best suit and protect our customers needs.

We all are, work in progress when comes to cybersecurity upgrades. This is because transformation isn’t a journey to a fixed endpoint, but rather a mindset of continuous improvement and growth. Hopefully, this is what 2022 holds for us all.

Energy Logserver Team

December 2021