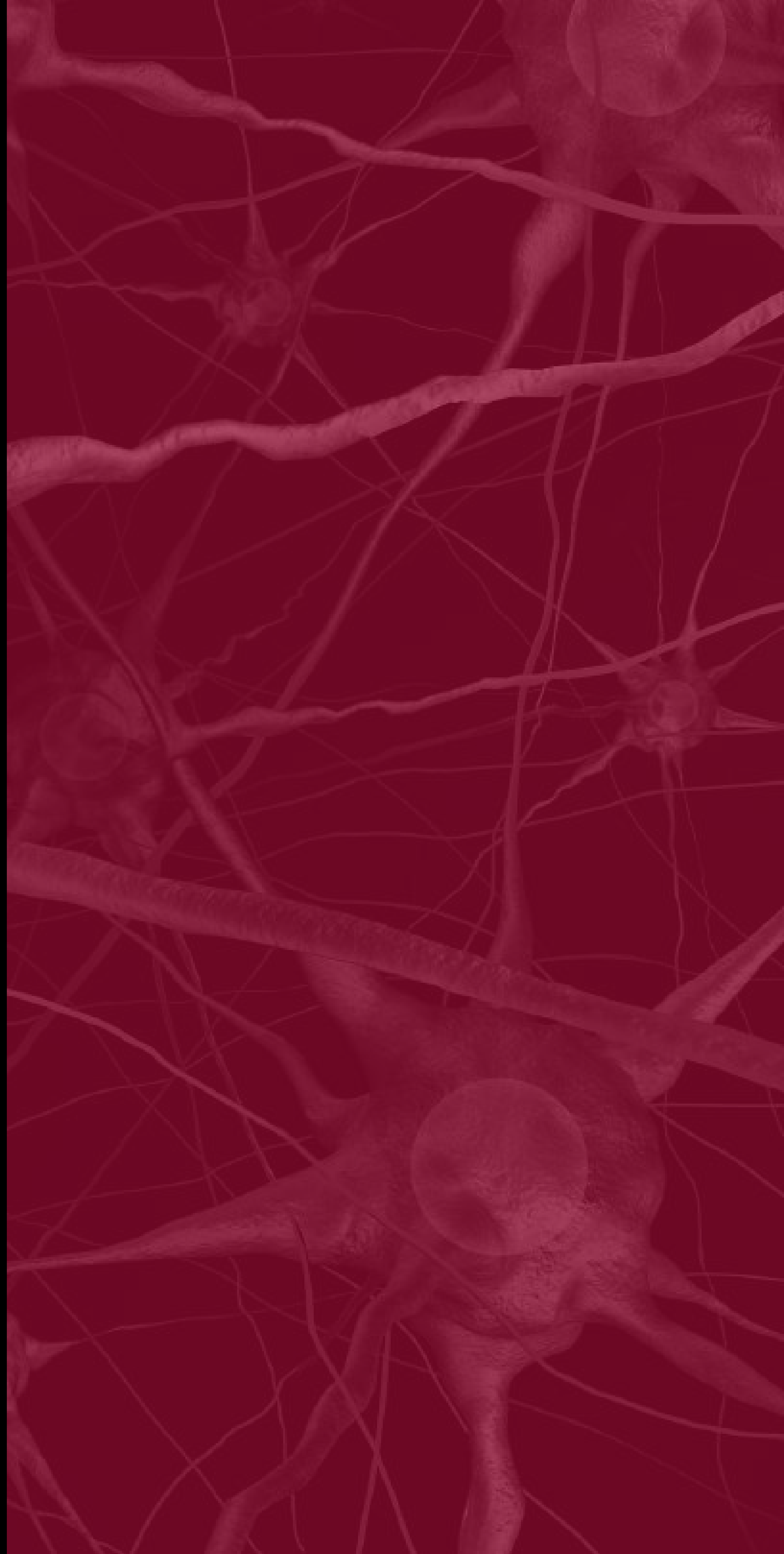
ENERGY LOGSERVER

CYBERSECURITY IN 2023

Report: BUSINESS AND CYBER THREATS

UNCERTAIN SITUATION FORCES QUICK REACTIONS

Cyberattacks have intensified as the conflict in Ukraine is escalating. The number of cyberattacks and their range have increased exponentially. The nature of incidents has also evolved, becoming more sophisticated. The pressure resulting from the unstable geopolitical situation has made it necessary for companies to respond quickly to changing conditions. As a result, the adoption of data-driven models and the growth of the big data industry continues, as more and more companies adopt data-driven models, recognizing the value of big data as a source of intelligent business decisions and change.



STAYIN' ALIVE

The way of doing business is rapidly changing. To survive in an uncertain environment, the modern organizations must react and adapt very quickly. The main challenge is the urgency to be always few steps ahead, especially in terms of defense against cyberattacks. However, managing cyberthreats has never been this difficult before.

BENEFIT FROM CONFIRMED DATA

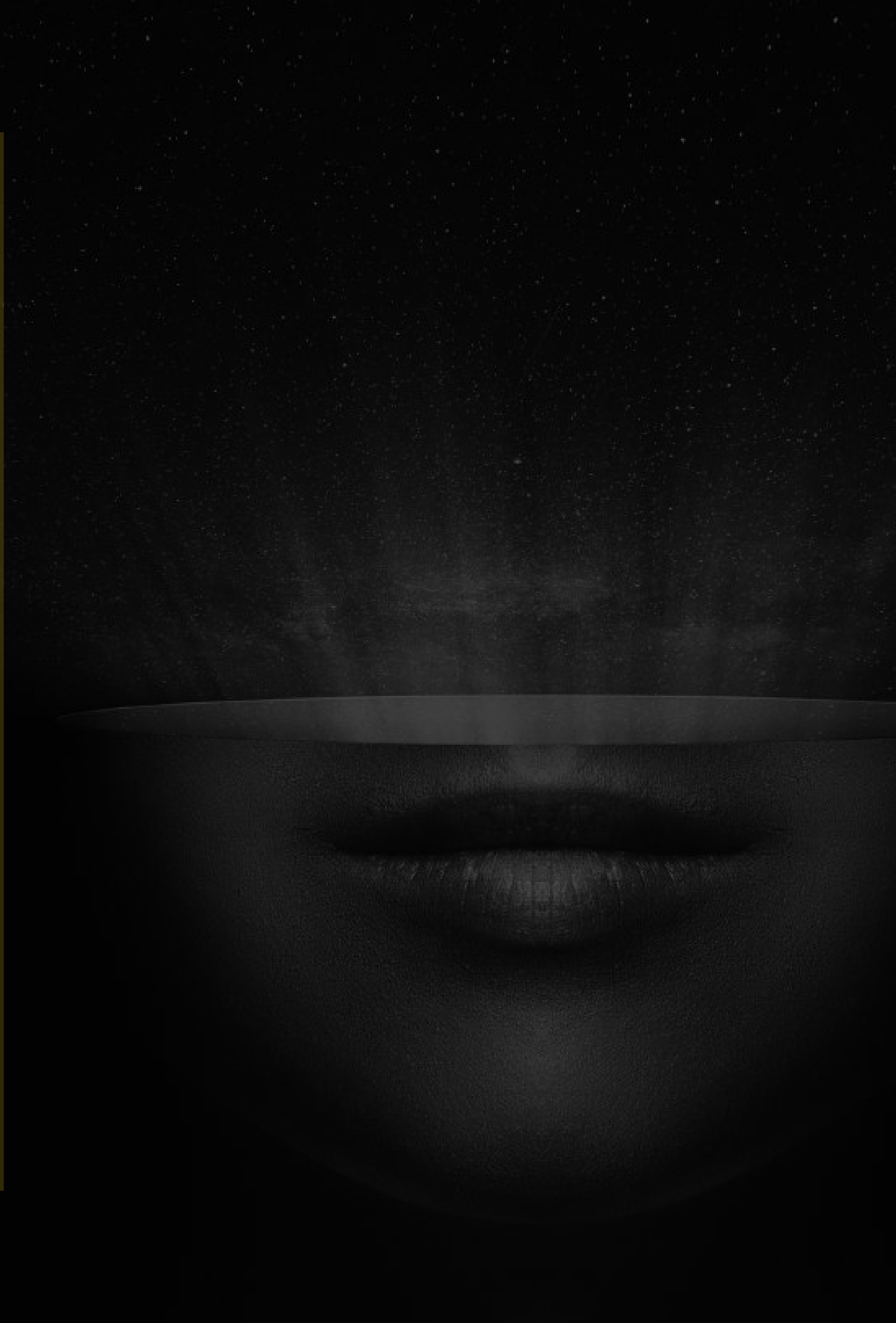
We can clearly see that big data is proving its value for organizations of all types and sizes and across many industries. In 2023, business decisions based on confirmed information will be the basis for the wave of digital transformation that organizations will experience. Companies that adopt a business model based on big data and use it effectively will be able to make informed decisions in an uncertain environment. In doing so, they achieve measurable business and financial benefits, from improving operational efficiency and better insight into rapidly changing environments to optimizing products and services for customers.

PROTECTING FROM DATA BREACHES

Data protection strategies used so far in organizations are no longer sufficient, which means that the number of data breaches is growing at a rapid pace. According to IBM's “Cost of a Data Breach 2022” report, approximately 83% of the surveyed enterprises experienced more than one data breach, with the highest cost of a breach of $4.35 billion. To protect themselves against similar incidents, organizations will therefore look for the most technologically advanced cybersecurity solutions in 2023. In particular, tools that allow real-time data processing will be preferable, as only the most up-to-date information empower a clear competitive advantage. In this context, the security analysis of big security data can be very helpful as it enables effective detection and neutralization of cyber threats.

AUGMENTED DATA IS KEY

The development of artificial intelligence (AI) and machine learning (ML) will increase the importance of innovative augmented data management processes. Augmented analytics is playing a revolutionary role in collecting, processing and sharing data by combining artificial intelligence and machine learning protocols.



FORECASTS FOR 2023

As result in the year 2023 more attention will be paid to categories such as data quality, metadata management and master data management. Companies will search for tools capable of the widest possible integration and with as many functions as possible. Functionalities such as real-time monitoring, detection of suspicious network movements, alerts, vulnerability detection, detailed current reporting and efficient analysis of the information provided allow to quickly respond to current actions and prevent threats in the future. Enabling more accurate forecasts and reducing the amount of time spent on repetitive work, AI will have the greatest impact on business analytics. Extended analytics will be used in the increasing number of areas, which will further increase its efficiency. The determinant of achieving a competitive advantage will be data certainty and the ability to make decisions quickly.

THE IMPORTANCE OF AUTOMATION

Companies will analyze data and draw conclusions much faster than would be possible manually. Therefore, process automation, which is one of the biggest drivers of transformation in the data environment, will become much more important. In particular, the automation of big data analytics is one of the most promising areas in 2023. Data automation and orchestration relieves professionals of repetitive tasks. Thus, it contributes to increasing the efficiency of management.

USING THE RELEVANT SOFTWARE

However, it should be remembered that automation should be carried out sensibly. For an organization that aims to improve communication, data handling processes, and work efficiency, it is crucial to select the appropriate automation tools and implement them effectively within the current IT environment. Only a tool that easily integrates with the organization's existing infrastructure and business processes will allow the organization to properly use large data sets and provide a market advantage.

Thanks to automation, enterprises will gain a wealth of information and predictive capabilities. Thus, they will be able to set business goals much more effectively, which will translate into generating profits while reducing costs.

TARGETING SPECIFIC TYPES OF COMPANIES

The year 2023 will certainly be full of many data security incidents. Cybercriminals will focus on optimizing ROI. Geo-targeted phishing, ransomware attacks, as well as those related to cloud security, IoT and artificial intelligence will increasingly affect smaller and/or less mature organizations. Healthcare and education stakeholders will be most often targeted, as well as those that store critical information: sensitive data and top expertise. Companies from these industries should therefore be prepared for organized attacks against them.

However, experience shows that such companies in their core business often do not have a dedicated IT department capable of effectively oppose cybercriminals, as large cyber budgets and having the right people are required for this purpose. It is predicted that 2023 will be a time when outsourcing of cybersecurity services will play a significant role. Companies will look for competent and experienced external partners with appropriate human and technological resources, which are able to provide comprehensive support in the field of efficient handling of security incidents.

THE NEED TO OUTSOURCE CYBERSECURITY SERVICES

TAKEAWAYS

The overriding factors affecting the market situation of business entities are data collection, analysis, and automation. Big data is a source of information about what is happening in real time in an organization's IT environment. It drives change in the way organizations process, store and analyze data. In addition, combined with technologies such as artificial intelligence, machine learning, automation, and analytics, they help determine the most effective actions to coordinate the defense activities of enterprises.

Understanding the existing state of infrastructure security, knowledge of currently available tools and vulnerabilities existing in the environment will help effectively protect the organization. An integrated threat overview and securing data lead to rapid response and effective countermeasures.

The above-mentioned threats and geopolitical conditions significantly affect the economy and the operation of enterprises as well as mid-scale companies. In this landscape of uncertainty, the fight against cybercrime is particularly difficult.

Effective security of big data is becoming a key factor not only to survive, but also to ensure a competitive advantage.

In response, Energy Logserver is continuously improving its products and services to address the challenges faced by our Customers.

Energy Logserver Team
December 2022