Hungary Cybersecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 100 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Hungary Cybersecurity Market is anticipated to grow with a CAGR of 6.5% during the forecast period. Ransomware and DDoS attacks are expected to increase further during the forecast period and even more targeted against large organizations in regions where the adoption rate for cybersecurity solutions is not as high. Also, ransomware-as-a-service offerings and their construction kits have been estimated to fuel this increase, particularly as an easy tool for novice or low-skilled criminals.

Key Highlights
The national and international contexts of cybersecurity have undergone significant changes due to the emergence of cyberspace, a new medium that has become a key factor in the 21st century. The Hungarian cybersecurity strategy aims at developing free and secure cyberspace and protecting national sovereignty. Additionally, it strives to safeguard the operations of the national economy and society, adapts technological advancements safely to promote economic growth, and establishes global collaboration in this area in line with Hungary's national interests. To create a proper strategic framework for domestic collaboration and coordination as well as for international cooperation, both texts were written with consideration for international examples, the significance of international involvement, and trends and problems.
The most frequent target in the corporate-institutional area, according to the most recent MS Digital Defense Report, is retail (13%), which is followed by the financial services sector (12%), manufacturing (12%), government administration (11%), and healthcare (9%). The Cyber Threat Resilience Team, run by T-Systems, a division of Magyar Telekom, has noted similar trends. Every day, the CTRL evaluates and looks into hundreds of possible IT incidents. In addition, it discovers tens of real occurrences that are reported to the parties concerned and thoroughly investigated. The CTRL has found that the relative isolation and the difficulty of the Hungarian language are no longer a barrier because criminals now employ linguistically skilled people to carry out the necessary background checks.
The majority of firms are vulnerable to DDoS assaults due to the dramatic increase in bandwidth use. According to Accenture,

organizations that previously had over-provisioned bandwidth to deal with potential DDoS attacks have begun to use it for remote employees. This has led to decreases in bandwidth available to defend against DDoS attacks. With most of the workforce telecommuting, DDoS attacks have a strong potential to cause operational downtime issues for organizations.
Hungary, businesses rely on a wide range of experts to protect their systems, personnel, and data. Since cyber threats are growing more quickly than ever before, businesses all over the world are battling to locate qualified individuals who can assist them mitigate these risks. For companies of all sizes and sectors, a cybersecurity workforce shortage continues to be a challenge. Today's cybersecurity positions are multi-faceted and increasingly diverse across specializations, companies, and industries, which is highlighted by the growing need for a wider combination of technical and non-technical abilities.

Hungary Cybersecurity Market Trends

Manufacturing Sector Expected to Adopt to Cybersecurity

With the introduction of Industry 4.0, the manufacturing industry has grown more open to cyberattacks as it moves closer to a digital transformation. As a result, businesses must realign their security systems for the industry. To improve overall operational efficiency and lower production costs, every manufacturing industry sector, including automotive, logistics, the many engineering disciplines, power systems, consumer goods, and chemicals, have embraced digital technologies. Due to the sectors' efforts to collect data and use it for analytics to prevent downtime and keep the industrial sector functioning 24 hours a day, M2M communication and networking have increased.
As a result of their need for connection, several businesses may be vulnerable to cyberattacks. The industry value chain depends on intricate, frequently interrelated digital assets and ongoing data exchange to efficiently complete any task. Cyberattacks actively target the industry. Although compared to other highly targeted industries like healthcare and banking, cyber defensive solutions are less developed.
An upsurge in cyber-related events linked to the control systems used to oversee industrial processes is being observed by several manufacturing companies. PLCs, embedded systems, distributed control systems, and industrial IoT devices could all be included in these systems. These control systems make up the operational technologies (OT) that enable facilities to function as a whole. While enhanced productivity, quicker detection and correction of quality issues, and improved cross-functional collaboration are all benefits of connection, they can also increase the smart factory's potential risks.
As smart factory initiatives continue to increase across manufacturers' global footprint, cyber risks are expected to grow. The cyber preparedness of many manufacturers is less mature than likely necessary to protect against current threats and new threats and vulnerabilities that digital technologies create. Moreover, according to Hungarian Central Statistical Office, Hungary's GDP from manufacturing climbed from HUF 2016417 million in the first quarter of 2022 to HUF 2047185 million in the second quarter.
Manufacturing enterprises should invest in a holistic cyber management program that extends across the enterprise (IT and OT) to identify, protect, respond to, and recover from cyberattacks. Organizations should consider these steps when building an effective manufacturing cybersecurity program: perform a cybersecurity maturity assessment, establish a formal cybersecurity governance program that considers OT, prioritize actions based on risk profiles, and build security.

Cloud Deployment Factors Expected to Drive the Market

The adoption of on-demand security services in the region is being driven by the growing recognition among businesses of the significance of saving money and resources by transferring their data to the cloud rather than creating and maintaining new data storage. Cloud platforms and ecosystems are expected to accelerate the pace and scope of digital innovation over the next

several years due to a number of advantages.
Further, in November 2021, A comprehensive range of AWS's products and services were being distributed by Ingram Micro Cloud via its reseller network in Hungary and Poland, as the company stated. The action strengthens the global offering of Ingram Micro's Cloud Marketplace, one of the most complete and widely used collections of cloud products in the world.
As IT service has shifted from being provided on-premise to being provided outside of a company's borders, security has been a crucial factor at every stage of the cloud adoption cycle. SMEs prefer cloud deployment because it frees them up to concentrate on their core skills rather than investing their limited cybersecurity funds in security infrastructure.
Security is a crucial component of cloud architecture since the use of public cloud services expands the organization's trust boundary outside of it. However, the widespread use of cloud-based solutions has made it easier for businesses to embrace cybersecurity procedures. As cloud services like Google Drive, Dropbox, and Microsoft Azure become more widely used and become an essential component of corporate operations, organizations must cope with security risks, including losing control over sensitive data. As a result, on-demand cybersecurity solutions are being more frequently implemented.
Additionally, as cloud-based email security services become more popular, so are services that are integrated with other security platforms like IPS and NGFW. This tendency is discouraging businesses from investing in specialized, on-premise email or online security solutions.

Hungary Cybersecurity Market Competitor Analysis

The Hungary cybersecurity market is moderately consolidated, with the presence of a few major companies. The companies are continuously investing in making strategic partnerships and product developments to gain more market share. Some of the recent developments in the market are:

October 2022: The EU Cyber Resilience Act was the first EU-wide law to place cybersecurity requirements on manufacturers. Manufacturers and developers will be held accountable for the security of connected devices under this rule, which will apply to hardware and software. According to the European Commission, the regulation will address two problems: the low degree of cybersecurity of many of these gadgets and, more crucially, the fact that many manufacturers do not give updates to address vulnerabilities across European regions.

Additional Benefits:

The market estimate (ME) sheet in Excel format
3 months of analyst support

Table of Contents:

Hungary Cybersecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 100 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-20
		Signature