Russia 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 Russia Cybersecurity Market is anticipated to grow with a CAGR of 11.13% during the forecast period. Cybersecurity is a critical issue for national security. It affects the public and commercial sectors and encompasses various concerns linked to national security, whether through terrorism, criminal behavior, or state and industrial espionage. Due to the growing IT technological innovation and the capabilities of cyber weapons that pose a threat to national security, the threat landscape is constantly shifting.

Key Highlights

Russia has been focusing on being a digital economy. By 2024, the government intends to fully implement a comprehensive digital transformation of the Russian economy and social sphere. The increasing data leaks in the country make it imperative to strengthen cybersecurity. Furthermore, according to Fortinet Cybersecurity Company, 80% of enterprise traffic is likely to be encrypted, and about 50% of attacks targeting enterprises are likely to be hidden in encrypted traffic to infiltrate networks, therefore employing HTTPS inspection as a requisite.

According to Maza, a Russian carding and fraud discussion forum announced that it had been breached, and hackers have leaked users' email addresses and forum credentials. Flashpoint, a threat intelligence firm, added that the hackers involved could be forum members of a law enforcement agency. A 35-page PDF file leaked on the dark web, with 3,000 rows of data, including alleged user information.

In addition, in January last year, the Russian Foreign Ministry and the Government of Iran signed a cooperation agreement on cybersecurity and information and communications technology (ICT). The agreement includes cybersecurity cooperation, technology transfer, combined training, and coordination at multilateral forums like the United Nations. The cyber corporation between Moscow and Tehran is focused on intelligence sharing and improving cyber defenses rather than sharing offensive capabilities.

The increase in remote connections augmented by work from home has increased the scope of cyberthreat. For instance, according to the IBM Security report 2020, 76% of the respondents mentioned that remote work would increase the time to identify and contain a potential data breach. Having a remote workforce was found to increase the average total cost of a data breach of USD 3.86 million by nearly USD 137,000 for an adjusted average total cost of USD 4 million.

Over the past few years, security systems have focused on making it difficult for attackers to reach critical data. Some say that even this has not happened. As a result, the ordinary user is increasingly wary of the security of the Internet. Solutions that may have worked a few years ago are irrelevant now. Organizations need several resources to identify and recover from cyberattacks and be highly prepared. In many cases, the organization might need to shut down its operations for days to recover from a breach or attack. In poor planning and inadequate infrastructure, the time to recover from an incident may be considerably high.

Russia Cybersecurity Market Trends

Cloud Segment is one of the Factor Driving the Market

The increasing realization among enterprises about the importance of saving money and resources by moving their data to the cloud instead of building and maintaining new data storage is driving the demand for cloud-based solutions and hence, the adoption of on-demand security services in the region. Owing to multiple benefits, cloud platforms and ecosystems are anticipated to serve as a launchpad for an explosion in the pace and scale of digital innovation over the next few years.

Security has been critical at each step of the cloud adoption cycle as IT provision has moved from on-premise to outside of the company's walls. SMEs prefer cloud deployment as it allows them to focus on their core competencies rather than invest their capital in security infrastructure since they have limited cybersecurity budgets.

Furthermore, deploying public cloud service extends the boundary of trust beyond the organization, making Security a vital part of the cloud infrastructure. However, the increasing usage of cloud-based solutions has significantly simplified enterprises' adoption of cybersecurity practices.

With the increased adoption of cloud services, such as Google Drive, Dropbox, and Microsoft Azure, among others, and with these tools emerging as an integral part of business processes, enterprises must deal with security issues, such as loss of control over sensitive data. This gives rise to the increased incorporation of on-demand cybersecurity solutions.

Additionally, the increased adoption of cloud-based email security services is driving the adoption of services integrated with other security platforms, such as IPS and NGFW. This trend is demotivating enterprises to spend on on-premise and dedicated email or web security solutions. The companies partnering to obtain the benefits of services like Security, compliance, risk, and privacy teams need visibility into their managed cloud databases' security and risk posture to identify, assess and address their overall data security posture and degree of exposure to data breaches.

Telecommunication is One of the Sector Adopting Cybersecurity

Distributed Denial of Service (DDoS) attack is one of the most standard types of direct cyberattacks. It could make a machine or network resource unavailable to its intended users by indefinitely or temporarily disrupting the services of a host in connection with the internet. These attacks can condense network capacity, swell traffic costs, disturb service availability, and even compromise internet access by hitting ISPs.

Communication carriers are in the middle of technological evolution. Software-Defined Networks (SDNs) are transforming network management, and cloud computing helps telcos scale for growth. But with these opportunities come risks. Telcos often open themselves to cyber threats since they are responsible for constructing and operating crucial infrastructure needed to communicate and store sensitive data. Skilled hackers and government agencies deploy advanced persistent threats that could

operate undetected. Communication channel components, such as edge devices, core network elements, and end-user services run on them, are often targeted.
The telecom sector is booming with opportunities for operators to transform their revenue models by introducing new and innovative digital services related to IoT, 5G, e-commerce, data, content, OTT communications, and mobile payments or managed services. The increased IT infrastructure components, such as desktops, servers, information systems, data centers, and virtual machines, further add to the demand.
For instance, 5G networks can be sliced into uniquely purposed slices, and each virtual network slice could demand unique security capabilities based on various usage scenarios. Security of 5G network infrastructure should also considerably evolve alongside the standard. Further, According to the Information-analytical portal of crime statistics of the General Prosecutors of the Russian Federation, In Russia, there were 249.2,000 fraud instances in 2021 that involved computers, mobile devices, the internet, or other information and telecommunications technology.
Telecom companies have made considerable leaps in security to protect their networks and customers. Still, their employees and executives remain highly vulnerable to having their accounts compromised, according to research from cybersecurity company SpyCloud. Also, the 11 telecom companies in the Fortune 1000 comprise the most vulnerable industry in the study, which is at greater risk than retail, banking, healthcare, and other industries. This factor shows the significant need for cybersecurity solutions in the telecom sector.

Russia Cybersecurity Market Competitor Analysis

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

In March 2022, Royal Philips, a global health technology provider, announced the expansion of its medical device cybersecurity services portfolio at HIMSS22. Philips is introducing Secure Remote Access Management Service, leveraging the broad security capabilities enabled by integrating SecureLink's critical access management and governance technology with Philips Remote Services' secure connectivity framework for technical and clinical support. The services benefit healthcare providers, including increased uptime, clinical performance, and advanced security to help protect access to their clinical solutions and medical devices.

In February 2022, Vice Prime Minister Mykhailo Fedorov said Ukraine launched an "IT army" to fight against Russia's digital intrusions. Ukraine has called its hacker underground to help protect critical infrastructure and conduct cyber spying missions against Russian troops.

Additional Benefits:

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

Table of Contents:

SCOTTS
INTERNATIONAL

Russia 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	2026-03-01
		Signature	