Argentina Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 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 Argentina Cybersecurity Market size is estimated at USD 1.58 billion in 2024, and is expected to reach USD 2.35 billion by 2029, growing at a CAGR of 8.29% during the forecast period (2024-2029).

The cybersecurity industry is gaining traction in this region due to the rising government initiatives increasing internet penetration across Argentina countries. Also, the expanding wireless network for mobile devices has increased data vulnerability making cybersecurity a crucial part of the organization. The rising cases of cyber attacks and regulations requiring reporting are driving the growth of the cybersecurity market in Argentina.

Key Highlights
-Argentine society is significantly aware of cybersecurity issues. Still, it may be more focused on economic instability and physical security as this is more relevant to personal and family risk of cybersecurity threats. Cybersecurity technology adoption in Argentina is two to three years behind more mature markets such as the UK, US, or Brazil. Moreover, the exchange rate fluctuations and the devaluation of the Argentine peso negatively impacted the adoption of cybersecurity and related technologies.
-Guidelines for cybersecurity incident response and recovery were released by the Central Bank of Argentina (the "BCRA") on April 16, 2021, under Communication A7266. The BCRA specifically pointed out that the rules are intended for financial institutions, payment service providers that supply payment accounts, and the infrastructures of the financial markets. The BCRA emphasized that the rules, however, can be applied by any financial system institution as well as information technology and communication service providers, among others, due to their broad nature.
-To update and improve the data privacy framework, in January 2019, the Agency to Access to Public Information (the enforcement authority in charge of applying the Data Protection Law and the Do-Not-Call Law) issued Disposition 4/2019, which

established a set of best practice guidelines for the interpretation and application of the Data Protection Law. The Disposition provides guiding criteria on (1) the right of access to personal data collected through closed-circuit television cameras, (2) automated data processing, (3) data dissociation, (4) biometric data, (5) consent, and (6) consent of minors.
-Financial and operational difficulties are anticipated to dominate the post-Covid period, which increased cyber threats in Argentina will also characterize. Regardless of their size, industry, or financial strength, all organizations are reassessing their budget and cybersecurity goals. There is a sense of shared urgency and a shift towards new models with integrated security, perimeter protection, automation, next-generation identity, and access restrictions. The culture of cyber resilience that exists today, where SMEs are bridging knowledge gaps, chief information security officers (CISOs) are raising awareness, and legislators are echoing cybersecurity concerns in political hallways, was discussed by experts as being the most crucial aspect.
-Insurers working to provide their customers with adequate cyber coverage must overcome a slew of challenges, such as the lack of historical data in case of an accident or loss due to natural calamity. In most cases, there is a lack of historical data, but the law also doesn't allow organizations to reveal cyber breaches other than those impacting consumer data. Therefore, a significant number of cyberattacks are left unreported. This deprives insurers of the data required to measure all the costs of cybercrime, making it difficult for them to derive effective cyber policies.

Argentina Cybersecurity Market Trends

Threat Intelligence and Response Driving Market Growth

- According to Microsoft, last year, the digital civility index in Argentina increased by one percentage point to a rating of 72 out of 100. This indicates that the perception of civility in the South American nation has slightly dropped in online settings. It is preferable to have a lower score because it shows less exposure to internet threats.
- Digital technologies currently lie at the heart of every industry. The increased automation and connectedness have revolutionized multiple institutions; however, they have also brought potential risks in the form of cyberattacks. Threat intelligence is the ability that enables organizations to mitigate these attacks. Further, rooted in data, threat intelligence primarily provides context, such as who is attacking, their motivation and capabilities, and what indicators of compromise in the system to look for, which primarily helps make informed decisions.
- Currently, multiple industries in the region face numerous challenges that include rising persistent and devious threat actors, a flood of data full of extraneous information and false alarms across different, unconnected security systems, and a shortage of skilled professionals. Some organizations have been trying to incorporate threat data feeds into their network. However, they need to figure out what to do with all the extra data, majorly adding a burden to the analysts who may not have the right tools to decide what to consider and ignore.
- A cyber threat intelligence solution primarily addresses these issues. Advanced solutions use machine learning to automate data collection and processing, integrate with the existing solutions, take in unstructured data from disparate sources, and then connect the dots by providing context on indicators of compromise and the tactics, techniques, and procedures of threat actors.
- These platforms also provide a central place for security analysts to aggregate threat data, analyze and enrich this huge data to make sense of it, and create and memorialize the threat intelligence processes to better respond to threats and mitigate risk. These solutions can also optimize these operations by combining automation and orchestration to increase the security team's speed and efficiency while also providing confidence and validation through human intervention.

Manufacturing Sector is Expected to Increase the Adoption of Cybersecurity

- Every sector in the manufacturing industry, including the automotive, the various engineering disciplines, power systems, the

consumer goods industry, and chemicals, have adopted digital technologies to increase overall operational efficiency and reduce production costs. M2M communication and networking have been on the rise due to the industries working toward data collection and using it for analytics to avoid downtime, keeping the manufacturing industry operational round the clock.
- Industrial equipment is built to last, with machinery being expensive, cumbersome, and costly to replace. Although IoT offers several positive facets to the industry, these innovations are often incorporated gradually within existing assembly lines, as gaps between legacy and modern industrial devices are prime targets for hackers.
- The workplace shift caused by COVID-19 has altered how work is carried out. With assembly lines being managed on the cloud or remotely, Internet usage increased exponentially. This transition, albeit necessary, was rushed due to the pace and intensity of the pandemic, leaving several companies needing to establish security guidelines for their machine operations.
- The convergence of operational technology and information technology impacts industrial control systems (ICS) security and supervisory control and data acquisition (SCADA) systems. The systems are exposed to increasing threats and targets for hackers involved in terrorism, cyber warfare, and espionage. Further, according to the National Institute of Statistics and Census, In the current year, industrial production in Argentina grew 7.6% compared to the previous year.
- Increasingly connected and automated industrial devices with wider networks of industry 4.0 offer broader surfaces for attack. Reliable industry 4.0 cybersecurity, smart manufacturing, and other industrial operations can help prevent the pipeline from stalling during an operation. Legacy devices do not have proactive real-time prevention and can serve as a foothold for attackers to propagate throughout the network. Older equipment augmented with connectivity generally needs more on-device monitoring capabilities to ensure IoT network security.

Argentina Cybersecurity Industry Overview

The Argentina 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:

- October 2022: A new Managed Security Service ProvidersProgram has been introduced by Check Point Software Technologies Ltd., a global provider of cybersecurity solutions, which reduces administrative hassles and supports a partner service-led approach. The program offers partners the capabilities required for complete XDR/XPR, MDR/MPR, events management, and SOC certainty while also supplying operational peace of mind, thanks to Check Point's market-leading prevention-first security operations suite, Horizon. The MSSP program enables partners to increase their profits while enhancing organizational security.
- July 2022: Cybersecurity provider Palo Alto Networks and market player in next-generation technology and IT services, HCL Technologies, announced an expansion of their partnership to offer combined solutions that support customers' safe digital and cloud transformations.

Additional Benefits:

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

Table of Contents:

Argentina Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 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	2026-03-04
		Signature