# Infrastructure Protection Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 120 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 infrastructure Protection Market is expected to grow at a CAGR of 6.3% for the next five years. One of the key factors fuelling the expansion of the market for infrastructure protection is the growing requirement to safeguard operational technology (OT) and Information technology (IT) networks across the globe.

Key Highlights
The current corporate environment is becoming more digital, and the number of targeted cyberattacks on vital infrastructure and IT systems is rising. For business operations, there is dependability on the availability and integrity of IT systems. The public and private sectors face new cybersecurity security risks due to the proliferation of connected devices.
Understanding a potential risk in a company would be aided by risk management. The study carried out by this risk management software would assist the business in adhering to specific guidelines to prevent future problems. Other factors influencing the market growth include increasing cloud-based security solutions to boost productivity and efficiency, increasing security and data breaches, and expanding leading companies' research and development capacities.
Infrastructures nowadays are interconnected with international digital ecosystems, enabling improved visibility, management, and general ease. However, the absence of adequate security gap analyses is one of the most challenging parts of managing infrastructures that interface with emerging technologies before, during, and after a digital transformation process. Due to their operating system's outdated design and the brittleness of their hardware and software architecture, control systems that operate within infrastructures are inherently vulnerable to today's sophisticated cyber operations.
Infrastructure security design risks must be protected using many layers of defense and various review phases. The procedures would help businesses continue operating without interruption, but they must choose security solutions that are fit for the growing threats. Organizations should work with the desired partner and select a technical program to produce commercial success.
Digital connectivity has become more valuable, and the COVID-19 pandemic has had a variety of occasionally conflicting

repercussions on the digital infrastructure industry. The relevance of multiple infrastructure systems and services in sustaining economic and social activity and enabling responses to unforeseen threats and challenges while creating a vulnerability risk has been highlighted by COVID-19.

## Infrastructure Protection Market Trends

### Significant Demand in the BFSI Sector

The banking sector, or the more significant financial services sector, is comparable to the brain of a country's economy. Every organization needs a safe and dependable banking experience to support its operations. It is crucial for banks to concentrate on all factors impacting the security and integrity of financial transactions, contracts, and services, given the significant role that this vital infrastructure sector plays in our lives.
There have been substantial technology advancements recently in the BFSI (banking, financial services, and insurance) sector. Most banking and insurance activities are now conducted digitally, and the BFSI industry is already processing enormous volumes of digital data from several sources. For cybercriminals, BFSI companies are among the most lucrative targets. Due to global cybersecurity regulations and the ongoing threat from hackers, a robust data protection solution is required to safeguard BFSI operations.
Because of the nature of their activities, banks and insurance companies frequently have a significant regional presence. This suggests they must follow several regulations and compliance requirements worldwide and in their region. There is a complication since data compliance differs across every continent, nation, and occasionally even state. By utilizing solutions that simplify compliance reporting and audits, BFSI firms can abide by the law. Choosing a micro-segmentation solution for BFSI firms may reduce the scope of IT and compliance audits.
Another crucial security procedure is safeguarding micro-segmented data centers across multi-cloud or bare metal systems. If critical financial processes are divided into secure settings, APTs (advanced persistent threats) and needless data exposure would be minimized. Implementing a zero-trust security paradigm that rigorously checks each person and device seeking to access resources is highly beneficial for BFSI firms. It aids in tracing the source of access requests as well. Implementing MFA (multifactor authentication) is also advised to guarantee that more than one authentication parameter is necessary to confirm a user.
Turkmenistan's internet users were the most frequently affected by financial malware in the previous year, with 8.4% reporting such instances. Afghanistan and Tajikistan were the two most targeted nations in the study, respectively, for users. Users in these nations made up 6.7% and 6.6% of the users targeted by financial malware, respectively.

### North America Holds the Biggest Market Share

Due to the increasing acceptance of infrastructure protection solutions and services across the country's many end-user sectors, the United States and Canada region is anticipated to be a significant market for the forecast period. Also, the United States of America has a substantial vendor base, which benefits the market's expansion.
The DHS's Cybersecurity and Infrastructure Security Agency spearheaded the United States attempts to safeguard its vital infrastructure. These elements are accelerating the country's infrastructure protection market expansion. The government and other relevant organizations have also implemented several measures to protect crucial infrastructure. Thus, the industry for protecting infrastructure in the United States is witnessing significant opportunities.
In several institutions, the United States government has deployed reliable cybersecurity measures. Cybersecurity units were created to decrease cyber-attacks, which may have resulted in grave damage to the country, and deterrent measures were carried out. The National Protection and Programs Directorate (NPPD) has also attempted to establish public-private partnerships

to improve the security and resilience of the country's physical and cyber infrastructure.
The United States of America is said to be a global digital hub. Further drivers include rapid technological advancements, a considerable shift toward digital transformation, a rise in SMB cloud adoption, the organization's robust investment in infrastructure protection and security measurements, and ongoing infrastructure and cyber security modernization across the country.
In June last year, a federal cyber security law of universal applicability intended to safeguard vital infrastructure was first read, marking a turning point in Canadian history regarding data protection. Until now, Canada's privacy law framework has been acceptable (if not exceptional), but there has yet to be much in the way of generally applicable laws addressing cyber security outside the privacy law regime. This would indirectly push the organizations to adopt infrastructure protection programs across the country.

Infrastructure Protection Market Competitor Analysis

The Infrastructure Protection Market is fragmented as it currently consists of many players. Several key players in the market are in constant efforts to bring advancements. A few prominent companies are entering into collaborations and expanding their global footprints in developing regions to consolidate their positions in the market. The major player in this market includes Honeywell International Inc., Kaspersky Lab Inc., Johnson Controls International, McAfee Corp., Rolta India Limited, and several others.

In November 2022, Honeywell released new operational technology (OT) cybersecurity solutions to help clients protect their industrial control systems and operations' availability, dependability, and safety. The products, which include an upgraded Cyber App Control dashboard and a new Advanced Monitoring and Incident Response (AMIR) dashboard, are meant to give enterprises 24/7 intelligent threat detection across the growing attack surface of their industrial control systems (ICS).
In October 2022, Kaspersky introduced a new version of Kaspersky VPN Secure Connection that dramatically improves VPN tunnel speed by 200% when compared to version 2020. While a VPN-for-routers function automatically reroutes every connected device at home, split tunneling allows customers to prioritize secure connection traffic for certain services.

Additional Benefits:

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

**Table of Contents:**

# Infrastructure Protection Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 120 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 | |