

# Anomaly Detection Market is Expected to Reach USD 8.80 Billion By 2027

*Anomaly Detection Market Size – USD 2.76 billion in 2019, Market Growth - CAGR of 15.3%, Market Trends – Escalating usage in software testing*

NEW YORK, NY, UNITED STATES,  
January 21, 2022 /EINPresswire.com/ --  
Increasing cybercrimes and rapid increase in generation of data volume is one of the significant factors influencing the market growth.



Reports And Data

The global [anomaly detection market](#) is expected to reach USD 8.80 Billion by 2027, according to a new report by Reports and Data. The escalating use of Internet of Thing (IoT) is among the major drivers of the anomaly detection market. The increasing usage of IoT has resulted in a rapid growth of threats and attacks, including denial of service, malicious operation, malicious control, data type probing, scan, spying, and wrong setup that may cause an IoT system failure. According to a research in 2018, about 15.0% of organizations have deployed artificial intelligence solutions, and it was estimated that approximately 31.0% would be incorporating AI solutions in the next year. Moreover, around 50.0% of organizations have observed an increase in fraud value since 2018; and nearly 25.0% of the lost revenues were never recovered.

The incidence of a data flow anomaly is frequently a sign of the presence of a programming error, and the detection of such anomalies may be used for the detection of errors and upgradation of software quality. Also, anomaly detection helps end-users to identify software bugs as soon as they occur, providing programmers new perceptibility into the behavior of the programs, including tracing hidden errors that corrupt the program's outcomes or identifying rare corner cases in the logic sequence of programs.

Key participants include IBM, Hewlett Packard Enterprise, Dell Technologies, Trustwave Holding Inc., Wipro Limited, Teradata, Cisco Systems, Symantec Corporation, SAS Institute Inc., LogRhythm Inc., and Securonix Inc., among others.

Get a sample of the report @ <https://www.reportsanddata.com/sample-enquiry-form/2954>

Clinical studies have demonstrated that most COVID-19 patients suffer from the lung infection. Even though a chest CT scan has been found to be an excellent imaging method for diagnosing lung-related diseases, chest X-ray finds extensive application owing to its faster imaging time and noticeably lower cost than CT. Anomaly detection with the help of AI can assist radiologists in examining the vast amount of chest X-ray images for efficient and reliable COVID-19 screening.

Further key findings from the report suggest

- By component, the anomaly detection solutions contributed to a larger market share in 2019 and is likely to grow at a rate of 14.8% in the forecast period. An increase in unidentified malware compromising internal systems, devastating DDoS attacks, and other threats evading traditional security have resulted in network monitoring solutions furnished with robust AI solutions called Network Behavior Anomaly Detection. This solution permanently monitors network traffic, analyzing connectivity to seek anomalies and expose suspicious behavior allowing a response to yet unidentified security threats untraceable by other technologies.
- By deployment mode, the cloud held a larger market share in 2019, owing to several advantages such as cost-effectiveness, data-backup & restoration, scalability, and faster deployment, among others.
- By application, intrusion detection held the largest market share in 2019. The market dominance of this method is owing to its ability to build models of normal network behavior that are then used to identify new patterns that considerably move away from the profiles. Such anomalies may represent actual intrusions or just new behaviors that are required to be added to the profiles.
- By the end-user, the manufacturing industry is projected to grow at a rate of 15.8% in the forecast period. In manufacturing systems, reduction in downtime is critical, and anomaly detection lets predictive maintenance for a decrease in downtime issues. Of late, machine learning is being applied to detect anomaly in manufacturing processes.
- The Asia Pacific region is estimated to grow at the fastest rate of 16.6% in the forecast period, attributed to the developing IT sector in the countries comprising China, India, and Japan, among others.
- In February 2017, Hewlett Packard Enterprise (HPE), a leading market player, announced the acquisition of behavioral analytics firm, Niara, to aid businesses to detect and avert cyber-attacks on IoT devices deployed in the workplace. Niara offers a solution that uses machine learning (ML) and big data analytics to identify advanced cyber threats that have breached perimeter defenses, including firewalls.

To identify the key trends in the industry, click on the link below: <https://www.reportsanddata.com/report-detail/anomaly-detection-market>

For the purpose of this report, Reports and Data have segmented the global commercial drones market on the basis of component, deployment mode, application, end-users, and region:

## Component Outlook (Revenue, USD Million; 2017-2027)

- oNetwork Behavior Anomaly Detection
- oUser Behavior Anomaly Detection

## Deployment Mode Outlook (Revenue, USD Million; 2017-2027)

- On-Premise
- Cloud-Based

## Application Outlook (Revenue, USD Million; 2017-2027)

- Intrusion Detection
- Fraud Detection
- System Status Monitoring
- Fault Detection
- Others

## End-Users Outlook (Revenue, USD Million; 2017-2027)

- BFSI
- IT & Telecom
- Government & Defense
- Manufacturing
- Healthcare
- Others

Request a customization of the report @ <https://www.reportsanddata.com/request-customization-form/2954>

## Regional Outlook (Revenue, USD Million; 2017-2027)

- North America
- Europe
- Asia Pacific
- Latin America
- MEA

Thank you for reading our report. We also offer customized report as per client requirement. Kindly connect with us to know more about customization plan and our team will offer you the altered report.

Tushar Rajput  
Reports and Data  
+1 2127101370

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/561188225>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 IPD Group, Inc. All Right Reserved.