FirstWave

IoT Monitoring: Providing Insights That Promote Growth

E-Book

IoT Monitoring: Providing Insights That Promote Growth

As The Internet of Things (IoT) has grown massively in recent years, transforming how we live, work, and interact with technology and each other. With ever-growing fleets of IoT devices connected to the internet, IoT management and monitoring tools have become critical to businesses with IoT deployments. And while both concepts are closely related, they each have their distinct place within the world of IoT.

IoT management revolves around coordinating and controlling the various devices in the fleet. In effect, it handles the configuration, deployment, and maintenance of these devices and manages the (sometimes massive amounts of) data these devices generate. IoT management solutions are designed to simplify managing large-scale IoT deployments, providing administrators with a centralized platform to monitor and control the devices in their fleet.

- Real-time device performance monitoring.
- Data trends analysis.
- Alerting systems for anomalies and issues.

As such, IoT management is often seen as a more administrative function, while IoT monitoring is a more analytical process.

And while both IoT management and monitoring are crucial, this paper will focus on IoT monitoring. With a proper IoT monitoring system, organizations can optimize the performance of their IoT fleet, reduce downtime, and improve operational efficiency. We're going to look at the key components of a sound IoT monitoring solution. But before we do that, let's provide an overview of IoT management to clarify the differences.

IoT Management Overview

IoT management goes hand-in-hand with IoT monitoring. It involves overseeing the deployment, configuration, updates, security, integration, and troubleshooting of IoT devices. IoT management precedes IoT monitoring, and the latter depends on the former.

- **Deployment** is the first step in IoT management. It means installing and configuring devices and networks to establish an IoT fleet. This complex process requires careful planning to ensure that the devices are located in appropriate locations and configured correctly. You should also consider the types of devices used, such as sensors, gateways, and cloud platforms, and how they will communicate. Also, it's worth considering that in many cases, IoT management hinges on vendor-supplied software. Relying on such software means that administrators will need to wrangle though multiple software platforms to manage their fleet. Alternatively, you could choose a unified third-party platform, such as FirstWave, that brings different brands of devices together under a single umbrella to avoid "swivel chairing" and manage your entire fleet from a single centralized location.

- **Configuration** follows deployment in IoT management. Configuration within an IoT management solution ensures that devices are set up properly and perform as expected. This step handles the configuration of device settings, establishing communication protocols, and setting up data transfer mechanisms.

- **Updates** are also a big part of IoT management. You need to make sure your devices' software is up to date with the latest features and security patches. That means updating devices' firmware and software and ensuring your hardware is compatible with new software releases.

- **Security** is another critical aspect of IoT management. Security within an IoT management solution entails implementing technical measures that protect the IoT network and its data from potential threats - things like securing networks, implementing access controls, and encrypting data.

- **Integration** involves ensuring that IoT devices and systems within your fleet can effectively communicate and work together. That means integrating -

IoT Management Overview

different devices, like sensors and gateways, and ensuring they can "talk" each other using standard protocols.

- **Finally,** we get to troubleshooting. Identifying and fixing issues that may arise within the IoT fleet is vital in ensuring devices function correctly and their data is collected and processed. This is achieved through diagnostic tools that identify connectivity problems, software bugs, hardware failures, etc.

IoT Monitoring

Let's now dive a little deeper into IoT monitoring. We're going to go over the five key features of a proper IoT monitoring solution:

- Performance monitoring
- Security monitoring
- Status monitoring
- Data monitoring
- Fault monitoring

Performance Monitoring

Assessing the efficiency and effectiveness of IoT devices and networks

Many organizations depend on large fleets of IoT devices for their day-to-day activities. As mentioned above, these fleets can include thousands, if not millions, of devices. These swarms of connected devices provide said organizations with an unprecedented amount of information and insights. But they need a way to harness it. And as the number of connected devices increases, complexity unavoidably creeps in. So it becomes crucial to monitor your IoT fleet and the networks they use to ensure they're operating as intended.

Performance monitoring within IoT monitoring solutions is critical for several reasons. It helps in identifying potential issues before they become significant problems. Monitoring the performance of IoT devices and networks makes it possible to quickly identify any issues that may affect your fleet (poor connectivity, slow response times, or high latency). This information can then be used to take proactive measures before these issues turn into major headaches.

Performance monitoring can also help ensure that your IoT devices and networks operate within your defined parameters. That's critical to any IoT fleet. Monitoring performance makes it possible to identify deviations from expected performance levels, which can then be investigated and addressed. Several key metrics can be used to monitor the performance of IoT devices and networks. Such as:

- **Connectivity:** The ability of IoT devices to connect to networks and other devices. Poor connectivity can result in slow response times and data loss.
- **Latency:** The time it takes for data to travel between IoT devices and networks. High latency can result in delays and poor performance.
- **Bandwidth:** The amount of data that can be transmitted over a network. A lack of bandwidth can result in slow response times and data loss.
- **Uptime:** The amount of time that IoT devices and networks are operational. Downtime can result in lost data and reduced productivity.
- **Security**: The security of IoT devices and networks. A lack of security can result in data breaches and other security issues.

Using an IoT monitoring solution to monitor a combination of the above key metrics enables organizations to identify potential issues, optimize performance, and ensure that IoT devices and networks operate as intended.

Security Monitoring

Assessing the efficiency and effectiveness of IoT devices and networks

The crux of security monitoring within an IoT monitoring solution is the ability to detect suspicious or malicious activity. This is typically achieved using security information and event management (SIEM) systems designed to monitor and manage security events from multiple sources, including IoT devices. SIEM systems can detect and respond to security threats in real time, minimizing data breaches and other security incidents.

Intrusion detection systems (IDS) are another path to security monitoring within IoT monitoring solutions. IDS systems are designed to detect suspicious or malicious activity on a network or device and alert the proper stakeholders. These systems can help identify and respond to security threats quickly, reducing the risk of data loss or theft and minimizing breaches through quicker response times.

Other security monitoring measures for IoT devices include network segmentation, data encryption, and access control. Network segmentation divides the network into smaller isolated segments, helping to reduce the impact a security breach could have. Data encryption means encrypting the data as it passes through the network, enhancing both privacy and security. And access control involves limiting access to IoT devices and data to authorized personnel only through tailored permissions (following the principle of least access).

By taking a proactive approach to security monitoring, businesses, and individuals can help to prevent data breaches and other security incidents, protecting their devices, networks, and data from external (and internal) threats.

Status Monitoring

Keeping track of devices' operational status

In the IoT world, status monitoring is crucial to ensure the proper and efficient operation of devices and systems. By keeping track of the devices' operational status, we can quickly identify and resolve any issues and ensure that the fleet operates correctly.

One of the main benefits of status monitoring is that it enables us to keep tabs on device states (whether devices are on or off). While that may seem minor, it can have a massive impact on the fleet's operation. If a critical device unexpectedly turns off, it could cause costly downtime.

Another important aspect of IoT monitoring is tracking device status (whether online or offline). In the overwhelming majority of cases, IoT devices are connected to the internet, and a loss of connectivity can have serious consequences. If a security system loses connectivity, for example, it may not be able to produce an alert in the event of a break-in. By monitoring devices' online status, we can quickly identify any issues with connectivity and take steps to address them proactively.

Aside from tracking whether devices are on or off, online or offline, status monitoring can also track other essential metrics. For example, we can monitor a sensor's device temperature to ensure that equipment is operating within safe parameters and not overheating. We can also keep track of the amount of data a device is processing, helping to identify bottlenecks and optimize our fleet's performance.

Automated monitoring solutions can use AI-powered algorithms to continuously monitor the status of devices and systems while providing detailed status reports. That allows organizations to identify trends and patterns to optimize performance over time. And given the size of some IoT deployments, just the sheer number of devices makes IoT monitoring a basic necessity more than a perk.

Data Monitoring

Reviewing the data transmitted and received by the devices to ensure accuracy and reliability

Another critical feature of IoT monitoring solutions is data monitoring. Given the increasing number of devices connected to the internet, ensuring that the data they transmit and receive is accurate and reliable is crucial. That's where data monitoring comes in.

Data monitoring involves reviewing the data devices in your fleet transmit and receive in real-time. It's a critical process because it enables organizations to identify any inaccuracies or errors that might crop up in the data. Data monitoring ensures that the data is reliable and that decisions based on that data are accurate and sound.

Data monitoring also helps to prevent data breaches. With the number of cyber threats constantly increasing, it's critical to make sure your fleet's transmitted and received data is secure. Hence, data monitoring also has a security component, as it helps to identify any suspicious activity, and appropriate action can be taken to prevent any data breaches.

Data monitoring can also reduce downtime by monitoring your fleet's data and identifying potential issues that could cause downtime. The information gleaned can be used to take preventative action, avoiding (costly) downtime and ensuring that the devices continue to operate efficiently.

Last but not least, data monitoring is crucial in ensuring compliance with regulatory bodies. Given the increasing number of regulations governing data privacy and security, manually ensuring compliance can be daunting. Data monitoring can flag any areas where the devices are not compliant, and appropriate action can be taken to ensure compliance.

Fault Monitoring

Identifying and reporting on any failures or errors within the IoT ecosystem

Fault monitoring is the ability to identify and report any failures or errors within the network - and it can be the difference between a smoothly running system and one plagued with issues. Fault monitoring is especially critical to IoT fleets because of their scale and complexity. With so many devices and sensors connected to the network, it can be challenging to keep track of everything and be informed of any faults in the system.

One of the keys to effective fault monitoring is having a monitoring solution that uses machine learning and AI to analyze data across the IoT fleet. By analyzing data from the entire fleet, these systems can identify patterns and anomalies and flag potential issues. Once an issue is identified, the system can alert stakeholders and provide them with the information required to address the problem promptly.

Fault monitoring also includes a reporting component. IoT administrators need to be able to quickly and easily access information about any issues that arise within the fleet. So a user-friendly dashboard that provides real-time updates on the network's status at a glance will be mandatory. As will the ability to produce detailed reports on any faults or errors found.

On top of identifying and reporting faults, advanced monitoring solutions can also help administrators optimize their IoT fleet. They could, for example, flag devices that consume more power than necessary or sensors that provide faulty data. By addressing these issues, IoT administrators can improve the overall effectiveness of their fleet.

Real-world examples of the benefits of IoT monitoring by industry

So that's what IoT monitoring is all about. But the above lays it all out in the abstract. Let's now turn to some examples of how IoT monitoring can benefit different situations/ industries.

Retail: The retail industry can significantly benefit from IoT monitoring. IoT sensors help retailers track their inventory, monitor product displays, and follow the in-store movements of their customers, providing them with behavioral insights that can improve their bottom line. The information can also be used to optimize store layouts, improve product placement, and ensure product availability. IoT devices can also be used to monitor in-store temperature and humidity levels and ensure products are stored in the proper conditions.

Manufacturing Industry: IoT Monitoring can be used to monitor the performance of industrial equipment. By collecting data from their sensors, manufacturers can identify potential problems before they occur, reducing downtime and maintenance costs. It can monitor the quality of products, ensuring that they meet the required standards and the supply chain, to track the transportation of products from various suppliers to the manufacturing plant, ensuring timely delivery.

Healthcare: The healthcare industry is another sector that benefits from IoT Monitoring. IoT devices allow healthcare providers to monitor patients' health remotely, reducing the need for hospitalization. They can also be used to monitor patients' vital signs and track the movement of medical equipment and supplies, helping with care facilities' logistics and providing better medical outcomes.

Transportation: IoT monitoring can help transportation companies track their vehicles' movements to make sure they stick to the schedule. IoT devices can also monitor the condition of vehicles, reducing maintenance costs. They can even be used to monitor the condition of the roads to identify potential hazards and reduce the risk of accidents.

Energy: With the help of IoT sensors, energy companies have the ability to monitor their equipment's performance. They can monitor a home or business's energy consumption and identify areas where energy can be saved. Or it can monitor the condition of power lines to identify potential issues before they cause real problems.

Logistics: IoT Monitoring can also serve the logistics industry well. By using IoT devices, logistics companies are able to track their shipments in real-time to ensure on-time delivery to the correct locations. IoT devices can also monitor the condition of goods during transportation in an effort to prevent damage (and save money).

Agriculture: IoT Monitoring can be extremely useful in agriculture by helping farmers optimize their resources - think water and fertilizer. Farmers can determine when and how much water to use by monitoring soil moisture levels, reducing water waste, and optimizing crop growth. Similarly, farmers can determine when and how much fertilizer to use by monitoring soil nutrient levels, reducing fertilizer waste, and optimizing crop yield. IoT sensors can also monitor weather conditions, allowing farmers to make informed decisions about planting, harvesting, and other farm operations. For example, if a storm is approaching, farmers can quickly move their crops to a safe location and reduce their risk of damage and loss.

The Virgin Atlantic Example

Virgin Atlantic has used (and is still using) the vast amounts of information its IoT device fleet has collected from planes and passengers to redefine its brand.

Real-time crew performance, aircraft condition, and passenger experience information are collected and transmitted to cloud servers and end-user control applications. Whenever an anomaly is detected during a flight, a process is in place to ensure the necessary parts and tools are available at the arriving airport.

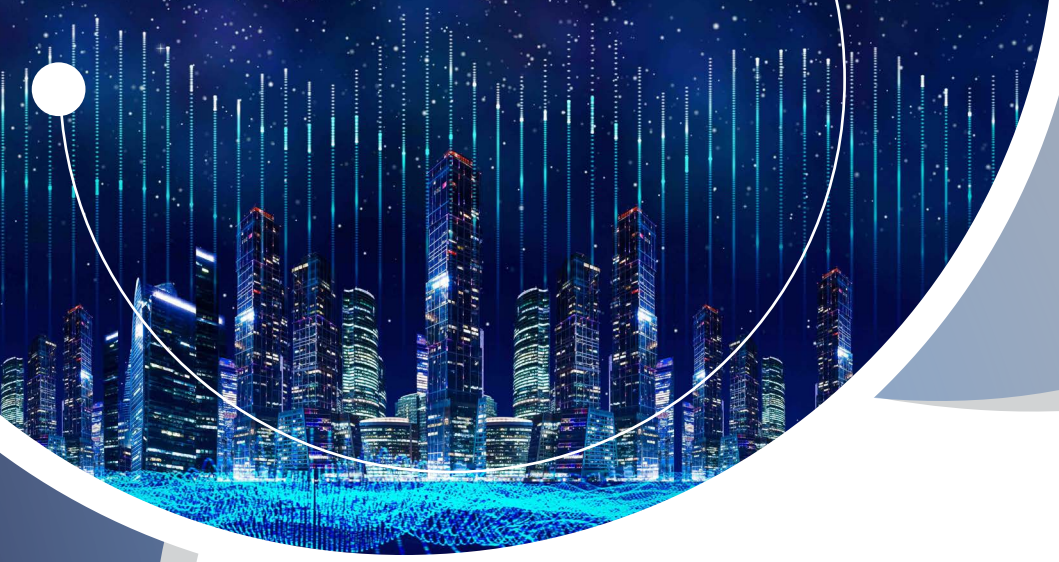
Virgin Atlantic's IoT-powered "Connected Engineer" project has led to a 20% decline in delays and an average turnaround time improvement of up to 30 minutes, according to Boeing, resulting in a 24% reduction in working hours.

Aside from enhancing operational efficiency, IoT monitoring is also helping Virgin Atlantic position itself as a sustainability-conscious brand. Air travel significantly contributes to rising energy demand and air pollution, and airline executives often find it challenging to present their companies as part of the solution. Virgin Atlantic has invested $1.4 billion to produce efficient jet engines, which employ connected technologies to adjust output based on weight

Get IoT Ready Solutions

CONTACT AN EXPERT

IoT monitoring has enabled Virgin to operate a shift in perception, not just for itself but for the entire air travel industry. That's the power of IoT monitoring.



Wrapping Up

So that was, in a somewhat deep nutshell, IoT monitoring—a critical tool for any business with an IoT component. The large-scale adoption of IoT devices has transformed how businesses operate and interact with customers. But as the technology landscape grows, business operations can become more complex. That complexity can be substantially mitigated by having a proper IoT monitoring solution tracking and reporting key metrics to stakeholders for informed decision-making. It also helps businesses identify areas for improvement and optimize their operations accordingly, leading to a reduction in costs, increased productivity, and better customer experiences.

Here are some of the key benefits of IoT monitoring:

- **It enables businesses to proactively detect** and troubleshoot issues before they become critical, reducing maintenance costs, minimizing downtime, and enhancing operational efficiency.
- **It helps businesses detect suspicious activities**, unauthorized access, and potential vulnerabilities in real time, allowing them to take timely action to prevent breaches.
- **It provides valuable insights** into the performance of the devices and networks, allowing businesses to gain a deeper understanding of their operations, identify areas for improvement, and optimize their processes for enhanced productivity and profitability.
- **It helps businesses to comply with regulatory standards** and guidelines by allowing businesses to track and monitor the data generated by the devices to ensure they meet the necessary compliance requirements.

By leveraging the power of IoT monitoring, companies can gain real-time insights into their operations, improve efficiency, and enhance their overall performance. Businesses can optimize their operations by investing in effective IoT monitoring solutions, driving growth and success. IoT monitoring provides organizations unparalleled visibility into their processes, so they can better understand their business and operations while making more informed decisions that lead to growth.

Wrapping Up

IoT monitoring can enhance the customer experience by using the gleaned insights to provide personalized services and products. IoT monitoring allows businesses to collect data on customer preferences, usage patterns, and behaviors to provide offerings tailored to their needs. This can lead to increased customer satisfaction, loyalty, and, ultimately, revenue growth.

IoT monitoring is a powerful tool that can help businesses stay competitive and thrive in today's digital landscape. It's a critical investment for any company that wants to stay ahead of the curve and succeed in the modern business world.

LEARN MORE

Does your organization have a proper IoT management and monitoring solution? FirstWave provides businesses with a centralized platform for both IoT management and monitoring that encompasses multiple vendor devices. Deploy multiple devices, anywhere, and manage them from a single unified platform.

FirstWave

Ready to level up?

If you need help with taking your IoT network management and monitoring to the next level, please contact FirstWave and we will be more than happy to help assess your current situation and recommend a solution to help your business.

CONTACT AN EXPERT

FirstWave

Our passion is to create intelligent software that our service provider partners and customers love.

Get Expert
Solutions

Book a demo

FirstWave is a publicly-listed, global technology company formed in 2004 in Sydney, Australia. FirstWave's globally unique CyberCision™ platform provides best-in-class cybersecurity technologies, enabling FirstWave's Partners, including some of the world's largest telcos and managed service providers (MSPs), to protect their customers from cyber-attacks, while rapidly growing cybersecurity services revenues at scale.

In January 2022, FirstWave acquired Opmantek Ltd (Opmantek), a leading provider of enterprise-grade network management, automation and IT audit software, with 150,000 organisations using their software across 178 countries and enterprise clients including Microsoft, Telmex, Claro, NextLink and NASA.

Integrating CyberCision™ with Opmantek's flagship Network Management Information System (NMIS) and Open-AudIT product enables FirstWave to provide a comprehensive end-to-end solution for network discovery, management and cybersecurity for its Partners globally.

With over 150,000 organisations now using FirstWave technology, we are well positioned to be a leader of transformational change in the IT Operations and Cybersecurity world.

firstwave.com | connect@firstwave.com