SOLUTION BRIEF

Ambient Conditions Intelligence Service

Solution Benefits

Plug-and-Play
Built-in Security
Extensibility
Distributed Monitoring
Cost Reduction

Use Cases

Remote Monitoring
Remote Management
Remote Update
Predictive Maintenance

The Challenges of Managing IT Infrastructure

The needs of IT infrastructure management in today's digital world are steadily increasing. Whether it is a large data center facility with thousands of servers, a small branch office with few racks, or a single outdoor enclosure with networking equipment, you need to have real-time insights of their operational performance. Maintaining availability and uptime requires not only monitoring the actual IT assets like servers and networking equipment but also the environment around them. Power, temperature, humidity, airflow from fans and cooling units, they all contribute to the factors that can bring your IT infrastructure down.

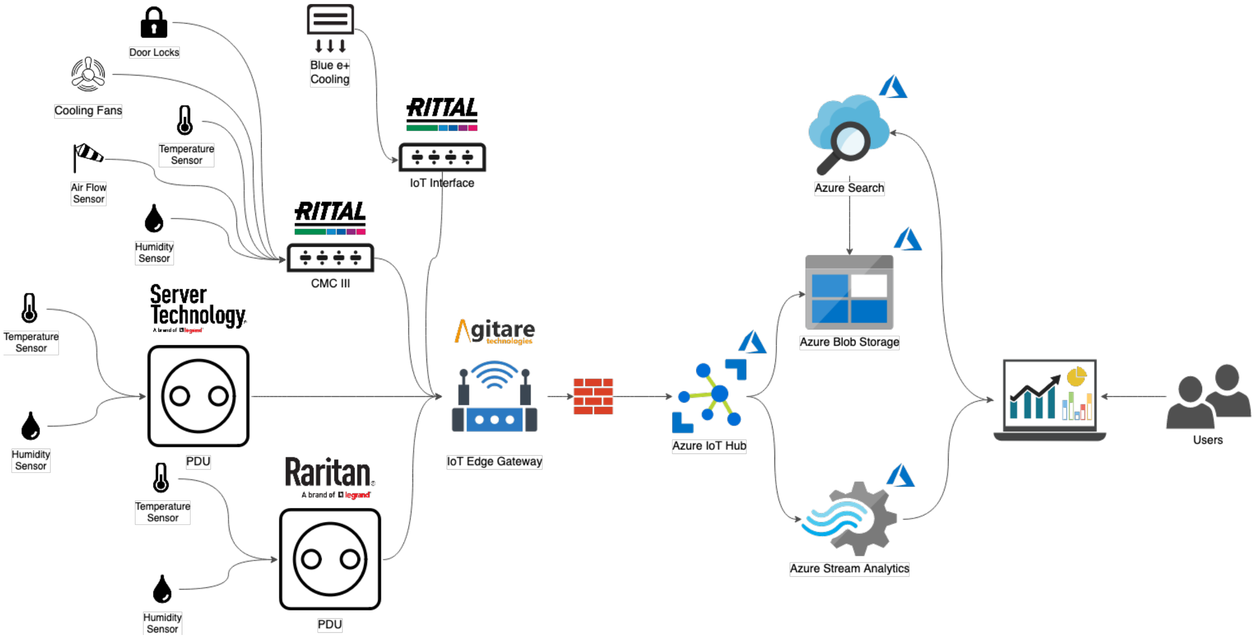
A myriad of vendors are present in today's IT environments, each one responsible for different parts of the infrastructure - enclosures, power, cooling. Each vendor offers capabilities for monitoring their equipment, but cross-vendor capabilities are lacking. On top of that, each vendor uses different technologies and approaches to provide monitoring information - legacy protocols like CAN/MOD bus, SNMP, or OPC/UA as well as modern gRPC and REST APIs. The promise of the DCIM solutions falls short because they bet on the common denominator protocols and cannot deliver on advanced features like cloud connectivity and predictive maintenance.

The use of legacy protocols also presents security challenges. CAN and MOD bus are specialized protocols intended for use in a closed system, while SNMP and OPS/UA have limited security features. Systems that utilize those protocols could not be exposed to the Internet without proper security. The lack of proper security and the inability to route those protocols over the Internet has traditionally constrained such systems to a single facility or physical location. Hence, the current DCIM solutions have a hard time offering a global view of the enterprise's IT infrastructure. Not only that, but the lack of data streaming capabilities like, for example, streaming log files, essential for servicing, and maintenance of infrastructure equipment required enterprises to implement costly point solutions using expensive hardware for remote access.

Last, but not least, the lack of standard automation approaches made the upgrade of such systems a tedious process involving expensive manual labor. That results in outdated systems, which additionally compromise security.

The Solution for Distributed, Cross-Vendor Edge Monitoring

Agitare Technologies, Inc's Secure Edge Monitoring Gateway enables enterprises to collect sensor and device data from different vendors and send this data to Microsoft Azure's cloud for reporting and analysis. The Secure Edge Monitoring Gateway connects to Azure IoT Hub using the MQTT protocol that allows it to communicate various types of monitoring data in a standard and secure way. AgitareTech's Secure Edge Monitoring Gateway can also be deployed with LTE or narrow-band connectivity to allow monitoring in the field or remote locations.



The monitoring data is stored in Azure Storage for a cold-path analysis and use in various scenarios like batch processing or machine learning. The data in Azure Storage is also indexed to enable search capabilities using Azure Cognitive Search. The same monitoring data is sent for a hot-path analysis to Azure Stream Analytics and visualized using Microsoft Power BI. The hot-path data gives the operations teams the ability to react to changes immediately and not wait for scheduled processing. Not only that, but the hot path can trigger automated processes and workflows.

The Secure Edge Monitoring Gateway also has log streaming capabilities that allow it to collect and stream log data from various vendor devices to Azure Monitor. The log data can use a standard Syslog format, but proprietary vendor formats are also supported.

AgitareTech's solution automates the set-up and configuration of the cold- and the hot-path, as well as the log streaming capabilities on the Edge. It also automatically deploys the required cloud infrastructure used to collect and process the data.

Solution Benefits

Plug-and Play

Agitare Technologies, Inc's solution is fully automated and can be deployed in existing or green-field Azure environments. The Secure Edge Monitoring Gateway requires minimal configuration of device IP addresses and can start streaming monitoring data immediately. The total deployment time for the solution can be reduced to a few hours.

Get fast insights with Microsoft Azure

Using Microsoft Azure's cloud technologies, enterprises can get fast insights from their IT environment. Whether it is visualizing the power consumption within a remote enclosure or the temperature variations between datacenters, searching the logs for relevant servicing information, or tracking the access to server racks, AgitareTech's solution can make it happen.

Extend with other vendors and metrics

Using Azure IoT Edge technologies, adding new vendors and metrics to AgitareTech's solution is a snap. With our help, you can develop and deploy new modules that collect monitoring data from other legacy vendors or internal systems.

Improve maintenance and time-to-repair

Having all this information at your IT team's fingerprints allows you to better plan maintenance schedules and reduce the time-to-repair of your equipment. Device log information is extremely valuable for the servicing personnel to determine the cause of failure and fix the device.

View and report across facilities

By using the power of Microsoft Azure, the monitoring and logging data can be submitted from anywhere. Remote locations do not require expensive remote access equipment to monitor and control. Leveraging LTE or narrow-band connectivity or standard Wi-Fi allows the AgitareTech's solution to collect data from anywhere.

Reduced cost of deployment and maintenance

Compared to the traditional remote access solutions, AgitareTech's Secure Edge Monitoring Gateway is a fraction of the cost. A single gateway can connect and control hundreds of devices across many enclosures. The ability to visualize the data in a single pane of glass reduces the need to sign-in to each device to monitor and troubleshoot.

Built-In Security

Unlike the traditional protocols and devices, AgitareTech's Secure Edge Monitoring Gateway is implemented with security in mind from the beginning. Each device is uniquely identified with a valid certificate and uses TLS 1.2 for communication to the cloud. A built-in firewall prevents outside access to the gateway and protects the legacy devices from malicious actors.

Current and Future Use Cases

Deploying the Agitare Technologies, Inc's Secure Edge Monitoring Gateway enables new monitoring and maintenance capabilities in the enterprises. Use cases can include but are not limited to

Distributed monitoring

So far, collecting monitoring and logging data from distributed locations has been problematic. Using AgitareTech's solution, enterprises can monitor equipment deployed in areas with wired, WiFi, LTE and narrowband connectivity.

Predictive maintenance

Monitoring and logging data collected from industrial equipment can be used to develop predictive maintenance algorithms. Those can significantly improve the mean time between failures and significantly increase the uptime of your IT infrastructure.

Remote management

Managing the equipment in distributed locations requires expensive remote access hardware and may pose security risks. With AgitareTech's solution, the enterprises can rely on an easy to use and secure way to manage their equipment from a central console. Re-configuring and restarting devices does not require multiple user-interfaces and exposure of numerous endpoints - it can all be done from one place with increased security.

Remote update

Upgrading industrial equipment software can involve manual labor, which makes it expensive and cumbersome. Quite often, such equipment runs outdated software that not only can cause outages but also compromises security. AgitareTech's solution can enable automated patching and upgrade of industrial equipment software and increase the uptime and security of your equipment.

Why Agitare Technologies, Inc.?

Our engineering team has a blend of skills ranging from hardware to the cloud to end-to-end security. Our experience in areas like cloud automation, software design, and cybersecurity allows us to build secure and intelligent IoT Edge solutions connected to the cloud. Our customers vary from large multi-national enterprises to small regional vendors.

T-Mobile relies on our data center monitoring solution to monitor the testing of its 5G equipment. Rittal uses our solution to assist its maintenance staff and improve the process for the extended warranty of their equipment. With our solution, Legrand can offer new services and insights for its ServerTech and Raritan PDU customers.

Our team does not only deploy the solution in your environment but also provides guidelines and best practices for configuration and management. For enterprises with limited staff or those who need to ramp up into the field, we offer affordable managed service.

Why Microsoft Azure?

Microsoft IoT platform is designed to deliver capabilities that support the core processes and requirements of various industries. It enables IoT solutions that seamlessly connect people, assets, workflow, and business processes, empowering organizations to be more resilient and agile.

Global Scale

With more than 60 regions and 170 global network points of presence, Azure has more coverage around the world than any other cloud provider—offering the scale and data residency options you need.

By deploying AgitareTech's ACIS solution on Azure, you can benefit from the low latency and high bandwidth Azure global network offers. As a customer, you maintain ownership of your data in the region of your choice. You are also in control of any additional geographies where you decide to deploy the solutions or replicate your data.

By using Azure services, AgitareTech's ACIS solution complies with local regulations and legal requirements.

True End-to-End Security

AgitareTech's ACIS takes advantage of the built-in security, visibility, and control enabled by Azure IoT platform. It prevents weak spots in your devices and services with security by design Azure monitors the health of all of your IoT devices in near real time and blocks compromised devices with Azure IoT Hub. Use Azure Security Center for IoT to find and eliminate threats with easy-to-follow steps ranked by importance, and configuration suggestions to help you improve your overall security posture.

With Azure, AgitareTech's ACIS gives you multiple layers of defense, continuous device monitoring, and the ability to return compromised devices to a safe state. With Azure IoT Edge and its extensible security framework, AI and custom logic is ran securely at the edge.

By integrating AgitareTech's ACIS solution with Azure Sentinel, you can find, investigate, and respond to the real threats in minutes without the fatigue of false positives. Azure Sentinel uses AI to make threat detection, investigation, and response smarter and faster.

Intelligence at the Edge

AgitareTech's ACIS solution leverages the power of Azure and Azure IoT Edge to built and train AI models in the cloud and run them on-premises. Anomaly detection and predictive models are deployed on the edge, and in case of an event, IoT Edge triggers an alert and processes the data locally or sends it to the cloud for further analysis.

Only a small fraction of IoT edge data acquired is meaningful post-analytics. By using services such as Azure Stream Analytics, AgitareTech's ACIS solution processes the data locally and sends only what's needed to the cloud for further analysis. This reduces the cost associated with sending all your data to the cloud while maintaining high data quality and operational efficiency.

With the help of Azure IoT Edge, you can operate your edge devices reliably and securely, even when they're offline or they have intermittent connectivity to the cloud. Azure IoT Edge device management automatically syncs the latest state of your devices after they're reconnected to ensure seamless operability.

Sustainable Future

Using Microsoft Azure is up to 98 percent more carbon efficient than using a traditional enterprise datacenter. Join the growing community of industry leaders that are reducing energy use and transitioning to a more carbon-neutral grid with Azure.

Microsoft has been carbon neutral since 2012 and is committed to being carbon negative by 2030, with the commitment by 2050 to remove all the carbon it's directly emitted since its founding in 1975. Take advantage of the lessons learned from Microsoft's own sustainability journey and help advance a low-carbon future—while you achieve your own sustainability goals.