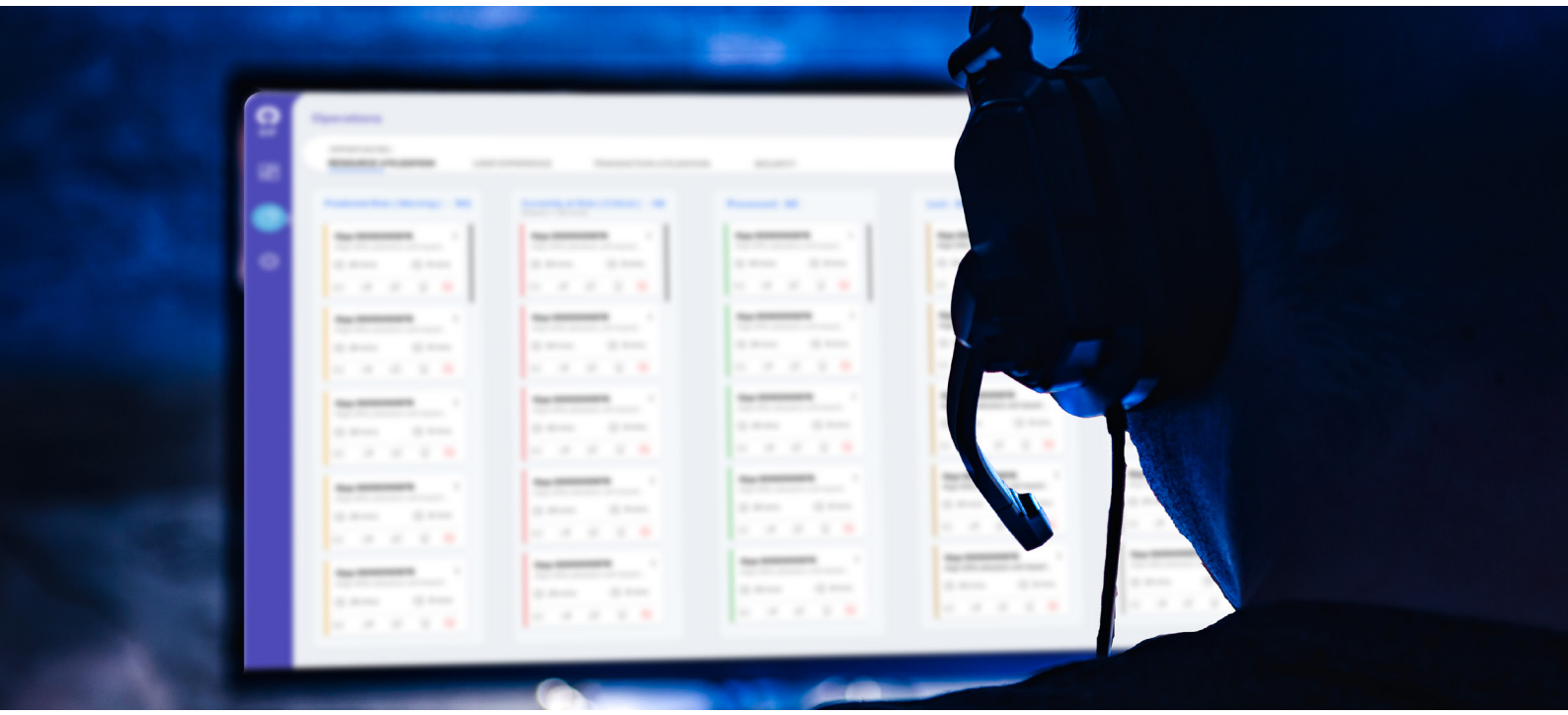


ZIF Monitor Data Sheet

Hear the unsaid
and feel the unfelt

Is your end user happy?

Your user could be using applications, services, servers and components of IT environment directly or indirectly. The application or service could be anything, from desktop applications, web or cloud-based applications on SaaS, to PaaS/ SaaS-based web services like payment gateways, APIs, etc. But is your end user satisfied?

User experience is a journey that is based on factors like speed, performance, flawlessness, ease of use, security, proactive attention and many more. Every business wants a happy customer; and business growth is directly dependent on the end users' experience and satisfaction.

End user dissatisfaction can heavily impact your goodwill as well as your revenue. Without monitoring or assessing their experience, you cannot determine whether a user is satisfied with your service.

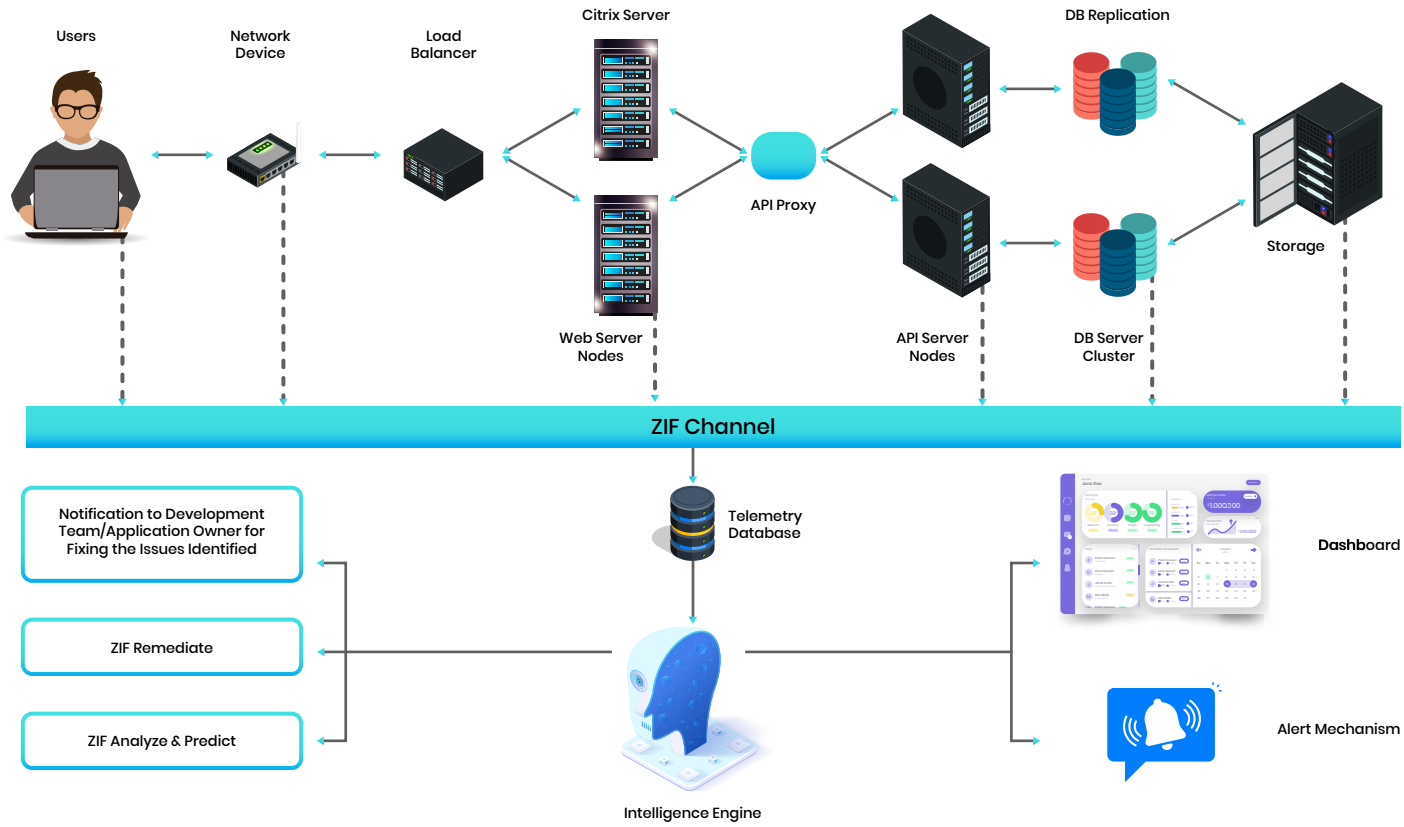
Turn your customer woes to wows!

It is important to have the right monitoring solution for an enterprise's IT environment. More than that,
it is imperative to leverage the right solution and deploy it for appropriate requirements.

We offer a unified monitoring solution for all your IT environment needs - ZIF Monitor. Its key objective is to improve user experience through real-time and proactive monitoring of IT environment.
ZIF Monitor is a component of ZIF™ - our AIOps tool that ensures business continuity using applications of ML, predictive analytics & automation.

The ZIF Monitor platform monitors all the layers involved in the user experience in real time. The layers that are monitored include but are not limited to - applications, databases, servers, APIs, end points, and network devices.

The figure below depicts the capability of ZIF Monitor to cut across all layers of IT landscape from end user to storage



Is your IT environment proactively monitored?

Environment Performance Management must move from being reactive to proactive. ZIF Monitor does exactly this for you through symptom and synthetic-based proactive monitoring.

The two phases of ML are Training and Inference.

Reactive Monitoring - When a problem occurs in an IT environment, it gets notified through monitoring and the concerned team acts on it to resolve the issue. The problem could be as simple as slow or poor performance, or as extreme as the unavailability of services like website going down or server crashing leading to loss of business and revenue.

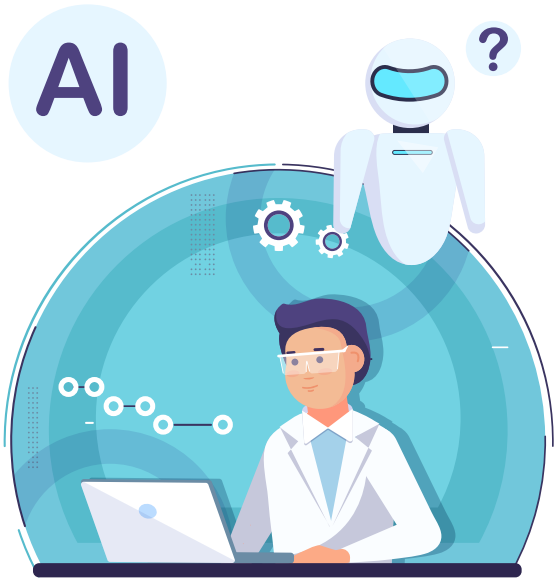
Proactive Monitoring - There are two levels of proactive monitoring:

Symptom-based proactive monitoring is all about identifying the signals and symptoms of an issue in advance and taking appropriate remedial action to nip the root-cause in the bud. This is the USP of ZIF Monitor.

For example, in case of CPU related monitoring, ZIF Monitor doesn't just focus on CPU utilization, it monitors the many underlying factors which causes the CPU utilization to increase such as processor queue length, processor context switches, processes that are contributing to high utilization and so on. ZIF Monitor not only monitors these symptoms, but also suggests remedy through the recommendation from SMEs.

Synthetic-based proactive monitoring is achieved through synthetic transactions. Synthetic Monitoring is done by simulating the transactions through the tool without depending on the end-user to do the transactions. The advantages of synthetic monitoring are:.

- Automated transaction simulation technology
- Round-the-clock environment monitoring
- Validation across different geographic locations
- Options to choose the number of flows/transactions to be verified
- Proactive – identifies performance bottlenecks or failures much in advance even before the actual user or the dependent layer encounters the situation



Highlights

- Unified solution for all monitoring needs
- Endpoint compliance and self-healing
- Agent and Agentless Solution
- Auto discovery – Servers & Databases
- Auto scale
- Auto upgrade
- Real user and Synthetic Monitoring
- Black box Monitoring

Offerings

Product

Infrastructure Monitoring: End-to-end monitoring of servers running Windows and non-windows. Non-windows include Solaris, AIX, Ubuntu, CentOS, RHEL, and SuSE

Database Monitoring: Monitors both RDBMS like SQL Server, Oracle, DB2, Postgres, MySQL) and NoSQL platforms like Riak, CockroachDB, Mongo, Cassandra, Neo4j, Redis

Application Monitoring: Monitors the performance and availability of web-based applications developed with .Net, Java, and Ruby

Containers & Microservices Monitoring: Monitors the availability and performance of containers and microservices

Outlook Monitoring: Available as intrusive and non-intrusive; monitors the end user experience and anomalies of Outlook

Service Monitoring: Available as intrusive and non-intrusive; monitors the end user experience and anomalies of Outlook

Process Monitoring: Monitors the availability and performance of processes/daemons which run in the background

Event & Syslog Monitoring: Monitors the content of Event log & Syslogs, raises alerts, and triggers action based on pattern match

Device Monitoring: Monitors the availability of devices connected through USB & COM Port

Web Server Monitoring: Monitors the health and performance of web servers like IIS, Tomcat

Synthetic Monitoring: Monitoring is done by simulating user transactions; helps to identify the anomalies proactively instead of waiting for user to face the problem and then act on it

URL Monitoring: Monitors the availability of web sites for its performance and availability

Log file Monitoring: Monitors the log file for any given pattern of value, exceptions or anomalies

Directory Monitoring: Monitors the directory or folder and raises alert when there are unintended files, files that are residing for a long period

Telnet Monitoring: Monitors the up-down status of Telnet port

Device Availability Monitoring: Monitors the availability of network devices or servers

Technology

Agent/agentless: Monitoring is done at the target environment like user devices, desktops, laptops, servers, network devices, load balancers, virtualized environment, API layers, Databases, Replications, Storage devices, etc

ZIF Telemetry Channel: Performance telemetry that are collected from source to target are passed through this channel to the big data platform

Telemetry Data: Refers to the performance and other metrics collected from all over the environment

Telemetry Database: The big data platform in which the telemetry data from all sources are captured and stored

Intelligence Engine: Parses the telemetry data in near real time and raises notifications based on rule-based threshold and as well as through dynamic threshold

Dashboard & Alerting Mechanism: The results of monitoring are conveyed as metrics in a dashboard view and as notifications

Integration with Analyze, Predict & Remediate Platform: Monitoring module communicates the telemetry to Analyze & Predict platform to use the data for analysis and apply Machine Learning for prediction. Both Monitor & Prediction platform communicates with Remediate platform to trigger remediation

Features and Benefits

Unified Solution

Platform covers end-to-end monitoring of the entire IT landscape. The key focus is to ensure all walks of IT needs are brought under thorough monitoring. Deeper the monitoring, stronger the outcome of journey towards incident reduction.

Agents with Self Intelligence

The agents capture various health parameters about the environment. They have inbuilt intelligence. When the target environment is already running under low resource, the agent will not task it with load, instead it collects the health-related metrics and communicates through the telemetry channel in an efficient and effective way. The intelligence is applied in terms of parameters to be collected, period of collection and many more.

Depth of Monitoring

Core strength of ZIF Monitor is that it comes with fully packed list of perfor mance counters which are defined by SMEs across all layers of IT environment. This is a key differentiator; the monitoring parameters can be dynamically configured for the target environment. Parameters can be added or removed on need basis.

Agent & Agentless

Solutions are offered both agent & agentless. It is easy for customers to choose. The remote solution is called as Centralized Remote Monitoring Solution (CRMS). Each monitoring parameter can be remotely controlled and defined from the CRMS. Even the agents that are running in the target environment can be controlled from the server console.

Compliance

Plays a key role in terms of the compliance of the environment. Compliance ranges from ensuring the availability of necessary services and processes in target environment; also, defines the standard of application version, make, provider, size, etc. that are allowed in the target environment.

Auto Discovery

Auto discovers the newer elements such as servers, end points, databases, devices, etc. that get added to the environment. It automatically adds these newer elements into the purview of monitoring.

Auto Scale

CRMS can auto scale on its own when newer elements are added for monitoring through auto discovery. The auto scale includes various aspects like load on channel, load on individual polling engine, and load on each agentless solution.

Real-time User & Synthetic Monitoring

Real time monitoring monitors the environment when the user is currently active. Synthetic monitoring is through simulated techniques. This doesn't wait for user to make a transaction or use the system. Instead, it simulates the scenario and provides insights to make decisions proactively.

Availability & Status of Devices Connected

Monitors the availability and control of USB and COM port devices connected.

Black box monitoring

It is not always possible to instrument the application to get insights, hence the black box technique is used. Here, the application is treated as a black box and it is monitored in terms of its interaction with the Kernel and OS through performance counters.

ZIF End User Monitoring

How ZIF uses End User Monitoring?

ZIF End User Monitoring, provides authentication to ensure the identity of user who uses the Laptop, Desktop, VDI. etc,. ZIF End Point Agent (EPA) tracks the productivity and monitors the resource availability like CPU, Memory, top resource consumers, top talkers via network

Biometric Authentication

ZIF End Point Agent (EPA) monitors identity of the user at end-point device and checks for user authenticity through biometric inputs at random or periodic interval based on the predefined configuration. This ensures the right user are using the end-point devices. The ZIF EPA resolves an authentication issue by immediately alerting the admin or performing a pre-configured action.

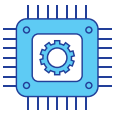
Productivity

ZIF EUM offers real-time insight into parameters that reflect user productivity. It monitors active and idle time based on mouse and keyboard usage, Application usage, NIC traffic pattern & usage, etc.

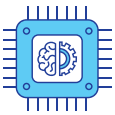
Unauthorized Device and Usage Detection

Unauthorized use (using banned devices, data capture, covering camera etc) can be detected based on behavioral patterns of use associated with a human being. Real time alerts are made.

Key Features



Resource Utilization:
Optimize resource utilization (CPU, Memory, Disk, Network IO)



Resource Optimization:
Discover available resource capacity across single or group of machines (CPU, Memory, Disk)

Productivity Measurement:
Monitor Mouse/Keyboard/App usage, Nic traffic

Software, License & Patch updates:
Get notified about software which are not required to be installed or outdated as per organization standards

Root Cause Analysis:
Identify processes (applications) consuming more memory, CPU, Disk

Compliance:
Gain insight into the unwanted application or process running at your end point

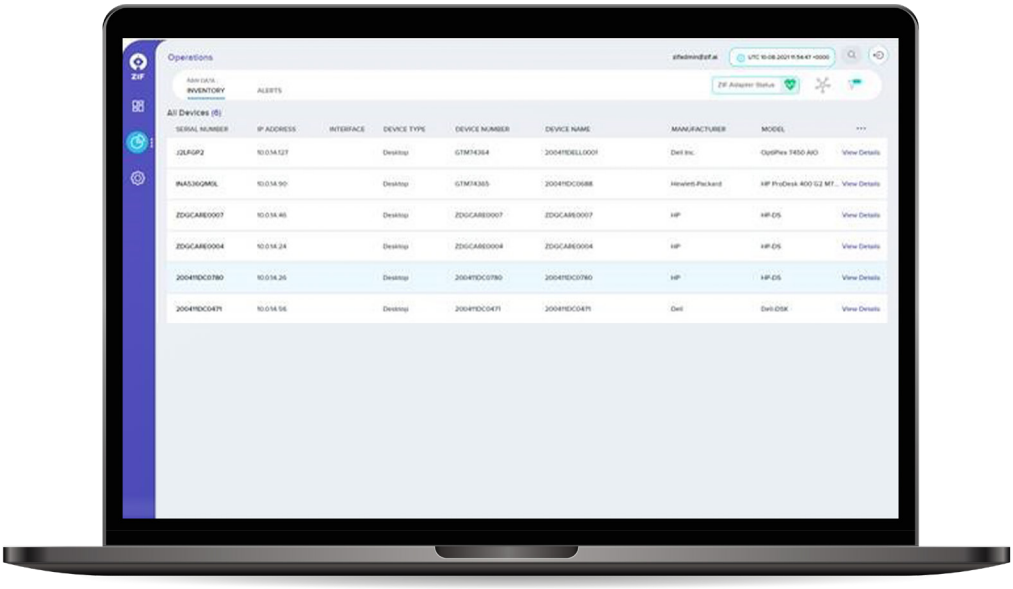
Application Inventory:
Understand the inventory of soft-ware installed on each end point

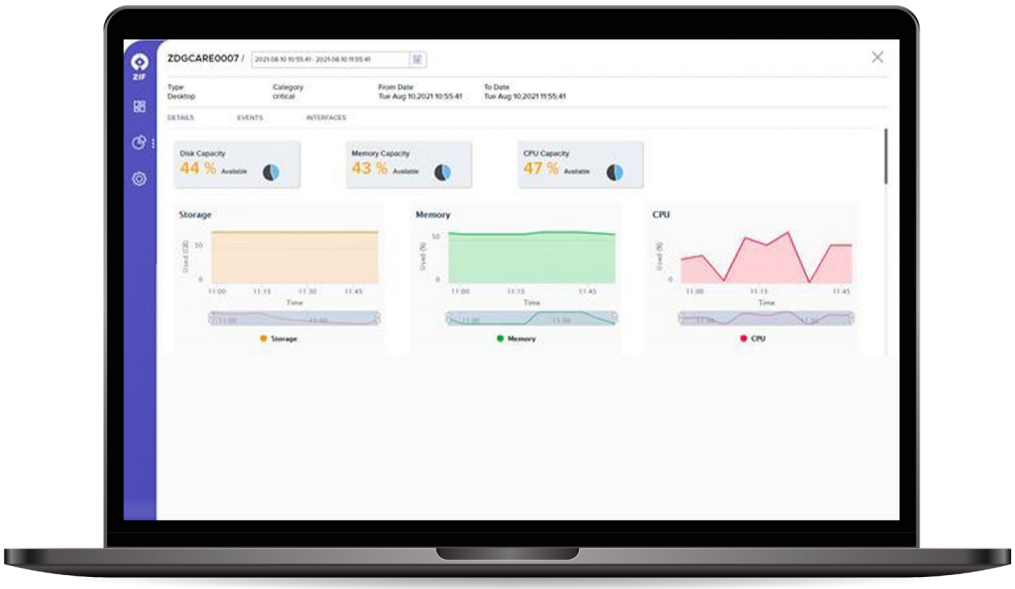
Ensure Essential Services Continuity:
Provide insights about the windows services & its status

Event Log Insights:
Get notified with the key windows events that are occurring at End point

End Point Utilization:
Discover the highly utilized end point and less utilized end point for a given duration (Typical for VDI users)

The figures below depict the ZIF End User Monitoring in action:





ZIF (**Zero Incident Framework™**), is an award-winning AIOps platform for IT Operations. ZIF delivers business outcomes by leveraging unsupervised pattern-based machine learning algorithms. Infrastructure and application telemetry data are aggregated, correlated, and potential failures are predicted. To enable faster resolution and better user experience, ZIF deploys intelligent bots for proactive remediation. Developed by GAVS Technologies (www.gavstech.com), ZIF is available as an on-premise and SAAS solution.

To find out how ZIF can help your organization, please visit **www.zif.ai** or write to **inquiry@zif.ai**