

MAG-UX

Visualize your performance & security

An Effective Failure Monitoring Solution
for IT Business Components





Performance Monitoring

Visualize your performance & security

Security Monitoring

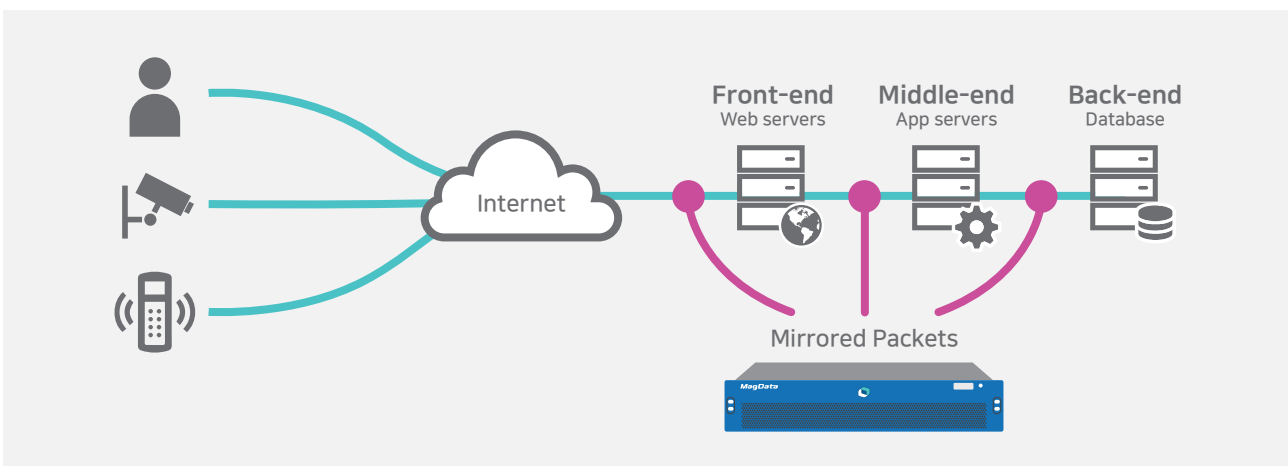


An Effective Failure Monitoring Solution for IT Business Components

MagData MAG-UX

In complicated and diverse digital business environments, it is very important to resolve failures on IT business components that could even paralyze an entire business. To do so, it is required to promptly diagnose and resolve performance and security problems in various IT components including applications, networks and servers. Especially, as IoT devices and infrastructures are growing rapidly, massive and diverse transactions from more complicated networks and numerous devices are increasing the likelihood of more IT failures. Moreover, an explosive number of devices and objects need to be monitored against those failures as there are more developments in cloud/data centers, home IoT, smart factory and smart city etc. Therefore, all companies having digital business components must be prepared technically to monitor and diagnose IT failures.

MagData's MAG-UX provides network-level diagnostics for performance and security failures, based on our technology in high-performance in-depth analysis of real-time mirrored packets. To do so, MAG-UX monitors the wire data of networks at L7 layer in real time, recognizes and analyses any IT failure promptly, and visualizes the status of all IT components in an intuitive manner.



<Figure 1> Failure diagnostics by sections based on high-performance packet analysis

※ **wire data** (Wikipedia, https://en.wikipedia.org/wiki/Wire_data)

Wire data is the information that passes over computer and telecommunication networks defining communications between client and server devices. It is the result of decoding wire and transport protocols containing the bi-directional data payload. More precisely, wire data is the information that is communicated in each layer of the OSI model.

Definition of Failure

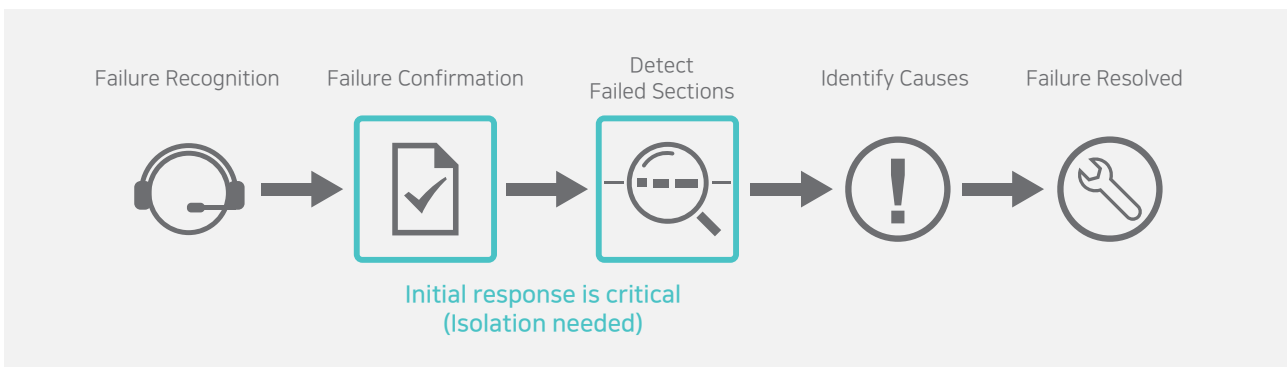
Typically, the cause of failures in IT business components is regarded as an unintentional failure in a performance aspect. For an example, a web server may not be able to handle massive requests from many concurrent users, causing transaction delays (latency) of more than 10 seconds, probably because of a program bug or a design defect. For another example, a central server can be overloaded by too many unnecessary transactions from IP cameras, probably because of a manager’s mistake. Those examples are considered as service failures in users’ perspective.

More precise definition of failures in IT business components can be classified into performance and security aspects, and those two aspects can be further divided into intentional and unintentional causes. Particularly, a cyber-attack, which is a typical cause of intentional failures, could incur severe performance degradation and malfunctioning.

	Intentional failure cause	Unintentional failure cause
Performance	Cyber-attack	System design error System operation error
Security	Cyber-attack Hacking	Manager’s mistake

<Figure 2> Classification of Failures in IT Business Components

MAG-UX can detect intentional and unintentional failures in both performance and security aspects, and provides visibility for real-time monitoring through intuitive interfaces. But, though MAG-UX provides functions to detect security failures, it may not replace traditional security solutions such as IPS.



<Figure 3> Process of Handling Failures in IT Business Components

Visibility and Intuitive Interfaces

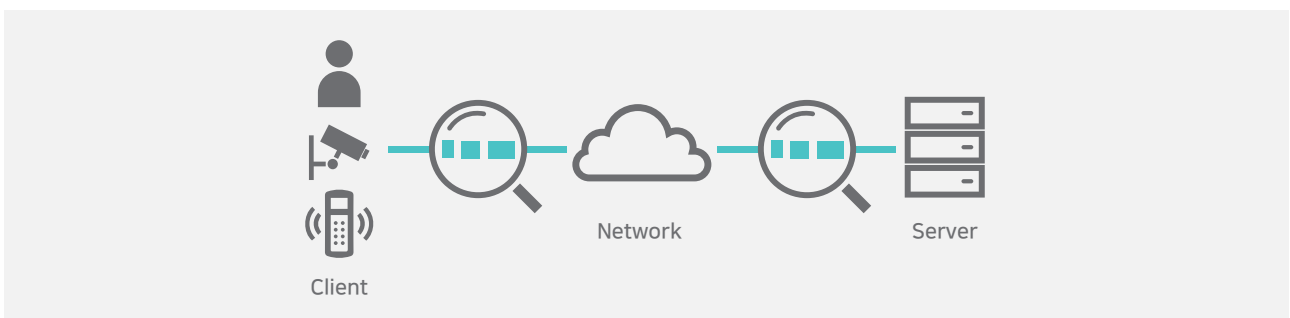
According to a report (“Magic Quadrant for Network Performance Monitoring and Diagnostics”, Feb 21, 2018) by Gartner, a top-notch IT consultancy, the goals of NPMD solutions should include not only monitoring network traffic and infrastructure to easily cope with faults and performance degradation of IT business components, but also finding out the opportunity of performance optimization. Also, the report indicates that many NPMD solution providers are entering the cyber security market as clients in security operations are having more interest in network traffic analysis. Furthermore, the report describes that NPMD’s functions of monitoring performance and security failures can be fulfilled by capabilities of diagnosis, analytics and root cause analysis.

To meet those demands in infrastructure monitoring, performance optimization and security monitoring, MAG-UX provides not only prompt warnings and alerts as soon as it recognizes any abnormal signal beyond certain thresholds by real-time monitoring, but also performance and security diagnostics in an easy, fast, highly visible and intuitive manner.



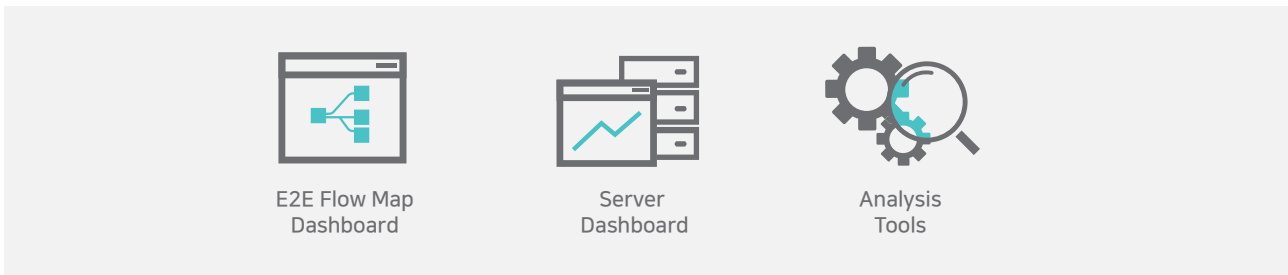
<Figure 4> Real-time processing by MAG-UX

Specifically, MAG-UX analyzes real-time status of each section, typically finer than a component, provides warnings and alerts, and recognizes any problematic section that can have a failure. Those features of MAG-UX can be realized by MagData’s switch mirroring technology that does not need an agent giving overloads to a server, not generate additional packets for monitoring, not adopt SNMP or a flow data method, both having difficulties in real-time processing, and not use a script injection method causing a potential security issue.



<Figure 5> Sectional processing by MAG-UX

Last but not least, MAG-UX provides various dashboards and real-time analysis tools to predict failure elements and their causes. These dashboards and tools facilitate a holistic “IT control tower” for performance and security diagnostics. We can tell that an IT control tower by MAG-UX has advantages in performance analysis/evaluation of IT service infrastructure, real-time monitoring, extensive analysis of network indicators, analysis across end-to-end sections, efficient decision-support tools, adaptation without adding failure elements, and intelligent anomaly detection.



<Figure 6> Monitoring functions of MAG-UX

Closing Remark

MagData Inc. has built our technological competitiveness in analyzing wire data that enables visibility and intuitiveness on end-to-end network data, with our company vision of “Visualize your performance & security”. Since we set network performance & security monitoring as our key business area in 2012, we have developed our flagship product, MAG-UX, to meet various demands from diverse customers. And our technology has evolved not just for client/server networks but also for hyper-connected IoT devices (MAG-UX for IoT). Currently, we are building a next version of MAG-UX to support trillion-level big data processing in a multi-parallel distributed architecture, and more advanced anomaly detection based on not just heuristics but also machine learning A.I. by analyzing massive real-time data. Therefore, we confidently propose that MAG-UX is a best solution for effective failure monitoring of IT components in your business environments

※ **NPMD** (Gartner, <https://www.gartner.com/reviews/market/npm>)

Network performance monitoring and diagnostics tools enable IT and network operations teams to understand the ongoing behavior of the network and its constituent elements in response to traffic demands and network utilization. Measuring and reporting on network performance is crucial to ensuring that performance stays at an acceptable level. Customers in this market are looking to identify tools to detect application issues, identify root causes and perform capacity planning.



MAG-UX

Visualize your performance & security

Function

Real-Time Processing

Sectional Processing

Diagnosis & Analysis

Feature

IT Control Tower

Port Mirroring (Agentless)

Transaction (L7) Analysis



Easy



Real-Time



Intuitive

MAG-UX provides performance and security monitoring of IT business components in a highly visible and intuitive manner, identifying service failures across end-to-end sections.

MagData Inc.

504, Pangyo 2nd Techno Valley Gyeonggi Enterprise Growth Center,
42, Changeop-ro, Sujeong-gu, Seongnam-si, Gyeonggi-do,
Republic of Korea (13449)

+82-(0)2.6121.8470

+82-(0)31.753.6767

magdata.net

contact@magdata.net