Unified Monitoring 101

A Guide To Monitoring The Entire IT Infrastructure

GROUNDWORK

Unified Monitoring is an integrated platform that monitors your entire IT infrastructure, including physical, virtual, and cloud. It's a proven strategy for reducing service outages, increasing end user and IT productivity, optimizing capital investment, and maintaining industry compliance. The business community has long recognized that productivity and profitability depend upon the smooth functioning of their entire IT environment, especially as IT infrastructures become more complex.

Understanding how and why unified monitoring works, and in what contexts it is most effective is essential. This report will provide a definition, basic foundation and value proposition for unified monitoring in the following sections:

I. Introduction
II. The Building Blocks of Unified Monitoring
III. The Business Value of Unified Monitoring
IV. Unified Monitoring: Use Cases
V. Key Questions and Best Practices of Unified Monitoring

Unified Monitoring Defined

At its core, unified monitoring means that all aspects of IT infrastructure are monitored for availability and performance, including: applications, databases, networks, virtual infrastructures, security systems, and special purpose devices. This universal coverage is unified by combining monitoring data from multiple tools for a complete picture of the performance and availability of the infrastructure. With a unified monitoring approach, you get visibility into metrics of interest from each of these discrete areas, while allowing the individual tools to perform their specialized functions, often with their own managers or teams of managers.

The overall goal of unified monitoring is to centralize the state of the entire IT infrastructure into a single pane of glass. A flexible and vendor neutral tool is important for this task, particularly one that is scalable and robust, yet simple to integrate.

As organizations evolve, many are moving to virtual and cloud-based servers yet still have a need to support their legacy systems. A good unified monitoring solution will provide coverage for both cloud-based and legacy infrastructures.

Unified Monitoring Is Needed Everywhere

FINANCIAL INSTITUTIONS

As financial institutions offer more diverse services to their customers, their infrastructure becomes more complex. Financial institutions are also uniquely challenged with increasing security threats and regulatory requirements. A unified monitoring approach can help financial institutions' IT departments centralize, making them more secure and stable, and allowing IT ops administrators to focus on overall system performance.

TELECOMMUNICATIONS

Uninterrupted service is absolutely crucial for telecommunication companies to maintain their reputation and retain loyal customers. Unified monitoring with network mapping, special equipment monitoring, and flexible detection of redundant data paths can help telecom service providers quickly identify and resolve their unique issues before problems reach their customers' attention.

GOVERNMENT

Security and cost are top concerns for government agencies with sensitive data to protect and taxpayer dollars to account for. Changing regulatory requirements are another area of concern. Unified monitoring that provides the necessary flexibility and integrates several performance tools can help government agencies meet compliance standards, improve security, and stay within budget.

HOSPITALS

Hospitals and related healthcare organizations have complex infrastructures that contain not only physical and virtual networks, but also thousands of medical devices connected to the network. Keeping track of all these devices is crucial to smooth operations and maintaining compliance, and automated network discovery and mapping tools are especially valuable in this environment.

EDUCATION

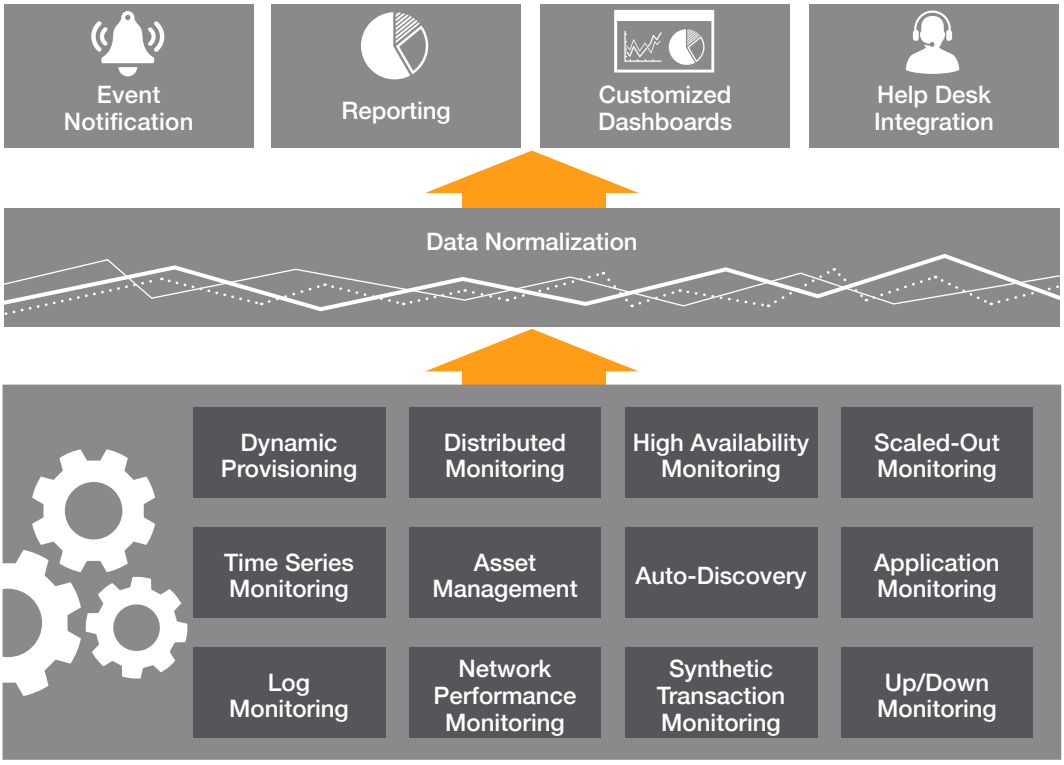
Many colleges and universities have multiple and dispersed IT departments, as well as special-purpose educational and legacy systems that need to be monitored, along with cutting edge virtual and cloud systems. These complex environments need a monitoring tool versatile enough to bring the entire IT infrastructure together.

The Building Blocks of Unified Monitoring

Unified monitoring combines monitoring data from multiple tools for a complete picture of the availability and performance of the entire IT infrastructure.

POWERFUL TOOLS EQUAL POWERFUL CAPABILITIES

The integration of several powerful tools is what sets unified monitoring apart. Powerful tools make capabilities such as event notification, reporting, customized dashboards and help desk integration possible.



The diagram above shows how multiple tools integrate to create one unified system that interfaces data flows to bring the necessary normalization, storage, and presentation systems together under a single user interface.

DYNAMIC PROVISIONING

Dynamic provisioning is the automated deployment of monitoring based on the deployed infrastructure—typically servers, virtual machines, containers, and componentized management systems. If you have VMware, for example, and you create a VM from a template, that VM should get added to the provisioned monitoring system without any special action from the administrator.

DISTRIBUTED MONITORING

Distributed monitoring is the collection of monitoring data from individual systems based on locally running a lightweight agent or other collection software. Simply put, distributed monitoring allows client systems to do part of the information gathering and transmission themselves. Agents can reduce the load impact on both the monitoring server and the individual systems being monitored. It is also more secure because the monitoring server is simply accepting data instead of actively connecting to individually monitored systems.

HIGH AVAILABILITY MONITORING

High availability monitoring is the provisioning of redundant, fault-tolerant systems to perform the monitoring function. Such systems can withstand the total loss of any one of a number of nodes without losing monitoring function. Load balancing, clustering, and replication technologies all play a part in making applications redundant.

SCALED-OUT MONITORING

Scaled-out monitoring is the ability to process large volumes of monitoring data into the system, typically by using multiple similar systems to handle the workload. Sometimes called horizontal scaling, this method can greatly increase the throughput of data into the system, and reduce latency when doing things like displaying and analyzing data.

TIME SERIES MONITORING

Time series monitoring is the ability to collect, analyze, and present performance metrics data over time. Most graphing systems show time series data by default (though there are also other ways of displaying data, such as histograms and pattern-based methods). Along with providing troubleshooting information, time series metrics can be used to drive long term capacity planning and investment decisions.

ASSET MANAGEMENT

Asset management is the ability to find and track equipment and software through its full life cycle. For example: where is that server? What rack is it in? What is its serial number? When was it deployed? Accurate dynamic provisioning requires some level of asset management data to be effective.

AUTO-DISCOVERY

Auto discovery is the process of finding and categorizing networked equipment for monitoring, and placing the discovered equipment into a topological structure or map. In some systems, asset-style data can be discovered, catalogued and stored along with availability and performance information.

APPLICATION MONITORING

Application monitoring is the collection of metrics as exposed by applications in APIs—for example, as JMX counters. These metrics can also come from more accessible sources such as log messages. Many developers have adopted monitoring libraries to make their applications easier to track and troubleshoot, and this is now considered a good practice in general.

LOG MONITORING

Log monitoring is the collection of log messages from systems and applications, and scanning them for error conditions. While this could be considered part of application monitoring, it is really more than that. Logs can be used in a very broad set of applications, such as security and intrusion detection, fault detection, access logs, audit logs and more.

NETWORK PERFORMANCE MONITORING

Network performance monitoring is the collection of performance data from network interfaces, typically via SNMP, and the associated analysis of this data to detect large or anomalous protocol spikes, traffic volumes, and error conditions. White the data that traverses networks is very large, sampling techniques like netflow or sflow can be used to characterize traffic patterns and QOS measures.

SYNTHETIC TRANSACTION MONITORING

Synthetic transaction monitoring is the periodic playback of recorded interactions with web-based applications and sites. Searching for terms in a database, for example, or placing orders in an e-commerce system and reporting any errors or anomalies in the performance of the transactions are typical cases.

UP/DOWN MONITORING

Up/down monitoring is the general collection of monitoring data using polling and plugin execution. If you need to know that a service is up, you would use this method to check it with as concise a test as possible. Another up/down use case is based on business service monitoring whereby clusters of checks are combined to represent entire lines of business with condensed single measures suitable for SLA reporting or dashboards.

The Business Value of Unified Monitoring

Unified monitoring impacts fundamental business objectives and drives business value. When your IT staff isn't spending time manually monitoring the infrastructure, they are free to accomplish profit-driving objectives. Additionally, with accurate capacity planning metrics, your organization can leverage existing IT investments and predict future expenditures.

Benefits of a unified monitoring system, include:

- Improved reliability
- Improved productivity
- Visibility into all aspects of IT
- The ability to craft meaningful SLAs and monitor compliance

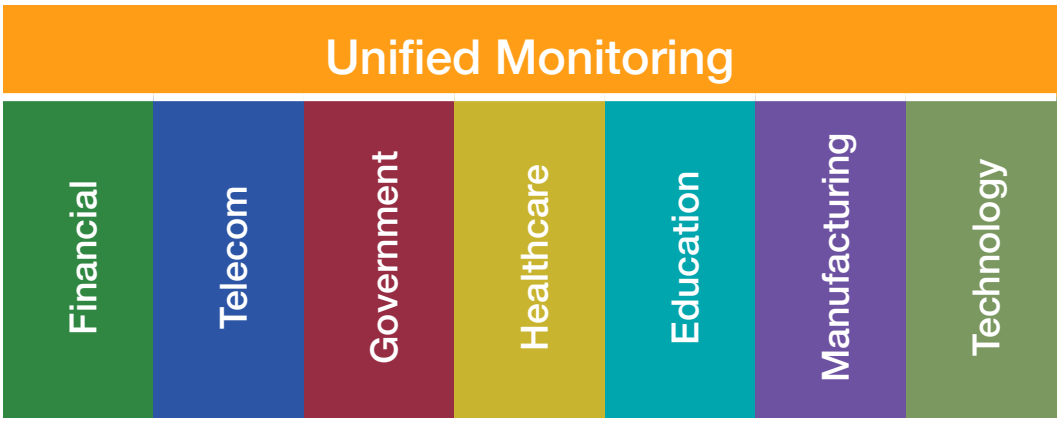
Mapping the Network

At its core, unified monitoring is all about providing a centralized view of the entire IT Infrastructure. This includes logical and topology mappings. It also encompasses deriving the dependencies between the monitored entities.

For example, one organization had a sudden issue with application latency in their environment. When asked, staff couldn't identify any changes to the environment that would impact latency. However, by looking at an automated network topology map, they were quickly able to determine that a device had been inadvertently added downstream of the application in a remote data center. This device was limiting communication to the upstream server, causing application latency. Because of this automated topology update, they were able to resolve the issue within minutes instead of hours or days.

The Audience for Unified Monitoring

Unified monitoring is for any organization that uses IT operations extensively in their business. Many times, the organizations who need unified monitoring have experienced outage and availability issues, have in-house solutions that struggle to scale or don't meet regulatory requirements, lack of visibility into their infrastructure, or don't have the ability to do reporting (for example: SLA compliance reports).



Wherever there is IT infrastructure, there is a need for unified monitoring.

- System and IT Ops Administrators need complete visibility into the IT infrastructure and an automated solution that lets them focus on their priority work.
- IT Managers need customizable metrics and performance indicators for reporting to executives.
- Capacity planners need accurate information to make budgeting decisions
- Executives need accurate information to make pertinent business decisions as organizations evolve.

> *You can't manage what you can't monitor*
>
> Thomas Stocking, Founder, GroundWork, Inc.

Business Use Cases of Unified Monitoring

With unified monitoring, organizations can take control over their IT infrastructure by exposing redundant systems, creating inventories of networked assets, identifying performance bottlenecks, standardizing procedures, and assigning role-based access.

SMOOTHING ACQUISITION

As businesses grow through acquisition, anticipated cost savings often comes from reducing duplicative infrastructures. There is a challenge with this approach when it

comes to IT, however, as IT systems tend to vary company to company in sophistication, age, specific equipment, and documentation. Additionally, staff reduction has left many companies with little visibility into their infrastructure as a whole.

Unified monitoring can expose redundant systems that are still operating post-merger, help create accurate inventories of networked assets, and document merged topologies that result from joining previously separate networks. Establishing standards for availability, performance, access controls, and tooling can smooth further acquisitions, and make SLAs feasible across the expanded enterprise.

For example, a distributor of commodities started as a small regional player, but gradually acquired several additional small distributorships throughout North America. The IT systems in these distributorships varied in size and sophistication from small single server local-area networks, to large warehouse control systems tracking extensive inventories. The company introduced a common inventory system, hand scanners, and standardized labeling and tracking, and centralized the data collection for billing, fulfillment and routing purposes. Large geographic separation led to latency in data collection, requiring distributed monitoring that was tolerant of periodic outages. Standardization allowed uniform metrics from applications used across the enterprise, and comparative statistics were used to highlight sites needing more resources or upgrades. Monitoring of the DR site allowed validation of redundancy and backups, creating resiliency of operations that could be verified without the experience of an actual disaster. Unified monitoring also covered the central data center, allowing efficient maintenance and response to outages. Recently, a cloud migration project was planned and executed for the data center. Monitoring in the cloud fed into the same unified system, letting the projected advances in reliability and performance be validated against actual, objective measures and compared to the legacy systems.

INCENTIVIZING PRODUCTIVITY

Companies often use metrics to drive decision-making at the management level, but one organization used metrics in an innovative way to make its DevOps team more effective. In one very critical area, availability and performance was key to the success of the business; literally, the faster business got done by this one team, and the more that was done in a day, the better the company did. There was no shortage of customers, and sales was actually constrained from adding more due to the capacity bottleneck this area represented.

Normally, simply adding people to a team that is a bottleneck is the go-to solution in this situation, but the managers were concerned that the required skill set was rare,

and the ramp-up time for new team members was long. Adding people was slow, costly, and of limited effect, so instead they decided to prioritize efficiency. Setting up a monitoring system that checked the throughput of the business systems, along with the availability of the API for accepting new transactions allowed the managers to place a clear set of numbers on a dashboard for all to see. They then paid bonuses on a monthly basis for the throughput measures. The team was left to devise ways to maximize throughput, and minimize downtime on their own, with a reasonable budget for equipment and software. The resulting innovations were a competitive advantage for years afterwards.

MANAGED SERVICE PROVIDERS

MSPs need to monitor infrastructure that they manage for their customers. While in any given IT environment there will be some variation, MSPs have an advantage: they can standardize and replicate the same basic environment for multiple customers, at least within limits. This has the effect of reducing the set of possible things that need to be monitored.

In some cases, an MSP may focus on a single application—for example, SAP. In this case, the monitoring best practices for SAP can be simply copies from customer installation to customer installation, and adapted to have larger or smaller footprints corresponding to the size of the customer installation. In other cases, MSPs may need to customize the monitoring system to cover exactly what they manage, and the components that let them do so, including networking switches, VPN servers, etc. Unified monitoring for MSPs therefore takes on a different context. Clean separation of customer data has to be balanced with the benefit of side-by-side comparisons that allow the MSP to best serve all their customers, and offer validated SLAs to them. Role-based access, flexibility, and standardized monitoring all help unify the monitoring in this situation.

Unified Monitoring: Key Questions for Best Practices

Now that we have a basic framework for unified monitoring, a solid best practices program begins with a set of key questions to consider:

SHOULD YOU USE A SAAS OR ON-PREMISE SOLUTION?

Some monitoring solutions are SaaS-based while others are on-premise, or offer both options. SaaS-based solutions are hosted on cloud providers like Amazon, or the vendor's own infrastructure. These solutions offer simplicity, but they also allow

data to leave the native network and be stored elsewhere. With an on-premise solution, you control the data on your own network. This is typically beneficial for organizations that need to protect their data or comply with regulatory standards. Knowing what is best for your organization is a key consideration.

WHAT TYPES OF NETWORKS AND DEVICES ARE IN YOUR INFRASTRUCTURE?

If you have a consistent hardware standard for network and server gear, or use private or public cloud computing, then you can expect a significant time savings to deploy your monitoring solution, and your best practice would be to select the monitoring that makes the most sense across the entire infrastructure first, and then layer on specialized options over this base. If, however, your network contains a wide variety of devices, is spread across multiple locations, or is only partially inventoried, then you would do best to run discovery tools first, sticking to basic monitoring until you have a clear idea of the various systems to be monitored. Then you can develop the specific measures to obtain, and roll them out to logical sets of systems (Linux servers on Dell hardware, then Windows servers, etc.).

DO YOU HAVE LEGACY TOOLS THAT NEED TO BE INTEGRATED?

Often there is some level of monitoring extant in the company already. Vendor specific solutions, in-house monitoring, and other related systems like configuration management or ticketing systems can all contribute data to the monitoring system, and should be considered for integration. For example, some companies run deployment on VMware from a CMDB, and have created user portals that allow quick requests for systems to be spun up, charged back, and added to monitoring with full automation.

WHO NEEDS ACCESS TO YOUR INFRASTRUCTURE?

Do you have multiple administrators with the need to access only specific systems? Can you logically group the systems needed so that the administrators need only manage the systems they are responsible for? If so, you can often delegate specific groups in LDAP/AD access to the monitoring on these logical groupings for monitored systems.

Do you need to plan for future capacity expenditures and perform trend analysis? Resource consumption can be tracked with monitoring systems (disk, RAM, cpu, etc), and these resources need to be understood clearly and measured in a standard way if capacity planning is the goal. Also, setting up results-oriented monitoring to correlate with resource consumption is a key way to obtain justification for future resource expenditures.

About the GroundWork Monitor® Platform

GroundWork Monitor® is a powerful on-premise unified monitoring platform that integrates availability, performance, and event data together with one-click access to related systems. With GroundWork Monitor®, you'll get complete visibility into your entire IT environment including physical, virtual, cloud, and hybrid infrastructures. If it's attached to your network, we can monitor it. GroundWork Monitor brings it all together into a single pane of glass.

QUICK AND EASY INSTALLATION

GroundWork Monitor® is easy to install. You can have it up and running in a few hours. The GroundWork team will help you implement your monitoring solution for maximum performance. Our goal is to make monitoring simpler so your team can focus on what you do.

FULL NETWORK DISCOVERY

Full network discovery automatically detects changes to your infrastructure. With drill-down topology mapping, you can quickly cut through thousands of events to get to the heart of an issue.

CUSTOMIZABLE DASHBOARDS

Customizable dashboards let you choose the information you want to see, and how you want it presented to others within your organization. You can assign role-based access and control each user's level of access.

OPERATIONS ANALYTICS

Operations analytics help you troubleshoot issues and plan for long-term capacity needs. With performance visualization, you can quickly spot problems and identify bottlenecks across your entire infrastructure. Log analysis helps you drill into specific issues to determine root cause.

About GroundWork

Founded in 2004, GroundWork delivers dynamic monitoring for dynamic environments with unified monitoring of hybrid cloud, container, application, server, network and storage data.

GroundWork's approach gives customers the flexibility to use diverse open source and proprietary software technologies together under a unified web services portal, allowing users to leverage the advantages of open source while simultaneously preserving existing investments in legacy IT management tools.

For more information, visit **www.gwos.com** to request a demonstration or no-cost trial.

www.gwos.com