Full-Stack IT Monitoring and Management Becomes a Strategic Imperative

Netreo™

Full-Stack IT Monitoring and Management Becomes a Strategic Imperative

Modern organizations simply can't function without a reliable, efficient, and always-available IT and networking infrastructure. Addressing this need requires a comprehensive management solution for the entire IT technology stack, from data center to cloud to network edge.

It's difficult to gauge what's increasing faster: the strategic importance of IT infrastructure, or that infrastructure's scope and complexity. No matter which trend claims bragging rights, the implication of the two in combination is inescapable: ensuring that IT operations are as reliable, efficient, and effective as possible has never been more important or challenging.

Organizationally, where there was once a clear dividing line between the IT department and the business operations it supported, the two are now inseparable. Our digitally driven and dependent world with its requirements for global interconnectivity and near-instantaneous responses simply couldn't function without a sophisticated, pervasive, and always-available IT and networking foundation.

That IT foundation has expanded dramatically from when servers, PCs, storage devices, and networking equipment constituted the vast majority of the IT hardware technology stack. Today, that stack also includes a wide range of mobile and embedded devices, Internet of Things (IoT) sensors, security tools, and a wide variety of other platforms.

Equally important, of course, is the stack and performance of software elements – from operating systems to enterprise applications to databases to analytics engines – that the hardware infrastructure supports.

Furthermore, during the past two decades, this increasingly complex and diverse IT technology stack has expanded dramatically beyond its original corporate building confines. IT infrastructures span from data center to cloud to network edge to end-user. The end-users themselves are equipped with ever-more capable mobile devices and pervasive networks, are often mobile, and due to the global COVID-19 pandemic, working from remote locations in increasing numbers.

IT managers charged with monitoring, maintaining, and optimizing the availability and performance of this diverse and dispersed infrastructure face a range of challenges. Among the most acute of IT manager pain points:

- Management and monitoring tool proliferation and fragmentation
- Alert overload and alert fatigue
- Manual processes that slow responses, add costs, and consume IT time and attention

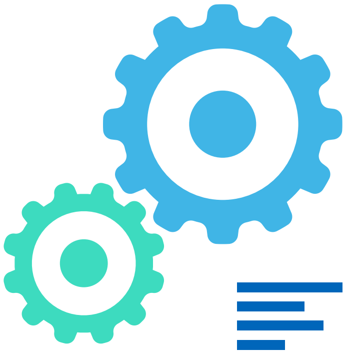
To ease these pain points, IT managers today require end-to-end visibility and control up and down the technology stack and across the distributed IT infrastructure landscape.

Integrating and Coordinating a Diverse Collection of Management Tools

To meet modern IT infrastructure challenges and demands, some IT monitoring and management companies are attempting to follow a similar playbook used by enterprise resource planning (ERP) vendors in years past. The strategy: grouping and integrating a wide range of discrete enterprise applications into tightly integrated application suites that share a common database.

Likewise, the goal of some cutting-edge IT management solutions is to unify as much of the infrastructure monitoring and management as possible under a common umbrella. Like their ERP cousins, the different elements of such a solution need to share a "single-source-of-truth" database that contains, in this case, performance readings, network traffic statistics, and a wide variety of IT events, alerts, and other operational data.

Providing such a comprehensive solution is no trivial task, given the proliferation of monitoring and management tools from a wide variety of vendors and the range of functions these tools provide. In many organizations today, individual solutions often aren't well integrated with other tools, resulting in operational silos that must be individually tracked and managed.



This fragmentation makes it difficult, if not impossible, for IT professionals to gain an end-to-end view of an organization's infrastructure and applications, understand the interactions and interdependencies of different elements, proactively spot emerging problems, or rapidly diagnose and fix any failures.

Among the most critical operational functions that a holistic monitoring and management solution must corral and coordinate include:

- **Server and back-end device management** – Monitoring, alerting, and reporting on server functionality, utilization, and potential or occurring issues.
- **Mobile management access** – Providing full visibility of the IT environment via remote access to the solution's interface and controls from a variety of mobile devices.
- **Network management** – Visibility into all network elements, both static and dynamic, with the ability to quickly drill into detailed information for troubleshooting.
- **Network traffic analysis** – Ability to consume and interpret data about network traffic flows, users, and applications to provide insight into how bandwidth is being used.
- **Cloud monitoring** – Providing insight into public, private, and hybrid cloud infrastructure elements and operations, as well as the user experience levels being delivered, with the same level of detail and context as if the infrastructure were on-premises.
- **Application performance monitoring** – Ability to ensure that applications are performing within required service level and user-experience parameters.
- **Configuration management** – Detecting, alerting, and reporting on any changes to device configurations with context and compliance awareness to help interpret the reasons and possible impacts of changes.
- **Database monitoring** – Monitoring of database performance metrics and trends, including alerting on unusual behaviors.
- **Reporting and analytics** – Seamless monitoring and reporting on all network-connected devices, systems, and applications with statistics and analysis presented in easy-to-understand reports and dashboard visualizations and without requiring scripting or SQL knowledge.

By tracking the interactions and interdependencies of these and other infrastructure elements, a comprehensive monitoring and management solution can help IT departments proactively identify and address emerging issues and immediately respond to any operational problems that do occur.

Identifying Critical IT Alerts Within a Sea of Operational "Noise"

Integrating and coordinating the wide range of monitoring and management tools and functions is just the first step organizations must take to address the challenges faced by IT departments. Unified or not, the broad and diverse collection of monitoring tools generates a tsunami of operational alerts that include everything from routine and repetitive events to configuration changes to device problems and failures.

Even mid-sized organizations can easily have thousands of infrastructure elements – both hardware and software – that collectively generate far more data than human analysts can absorb and interpret. The volume of alert "noise" can quickly result in alert fatigue with overloaded analysts unable to sort through the huge number of inconsequential, redundant, and false alerts to spot the handful of critical alerts that require immediate attention.

To help IT professionals navigate through the sea of operational alerts, a full-stack monitoring and management solution should provide a variety of useful capabilities. As a baseline, solutions should automatically generate an inventory of all of the devices active across the IT landscape. With this inventory in hand, IT managers can often identify non-critical elements that require no alert monitoring and simply eliminate the alerts those devices and systems generate from the overall load.

The monitoring and management solution should also help IT pros identify normal operational metrics for different elements of the infrastructure. Once known, these expected or required parameters would be used to set operational thresholds either manually or automatically. The system will then only pass through alerts when a monitored element begins to operate out of those established thresholds.

Ideally, the alert management solution will also identify the context of potentially anomalous operations, as well as the crossing of static thresholds. For example, a server operating at 80% of its capacity might be within its expected operational range. But if that same server is running at 80% capacity at a time of day when it normally runs at 20%, the alert management solution would trigger an alert that requires IT investigation.

Once the alert management solution identifies meaningful alerts, it should be able to direct alerts of different types to the proper IT professionals or departments for resolution. Ideally, IT managers should be able to configure the solution to automatically initiate fixes to problems that require instantaneous response. This and other types of monitoring and management automation collectively address the third IT management pain point – the inefficiencies, costs, and risks of manual operational processes.

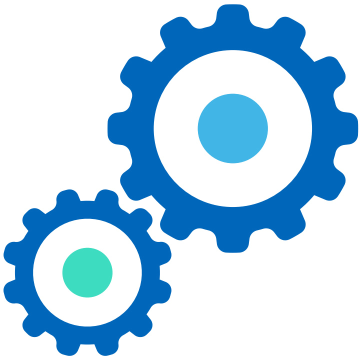
Optimizing IT Operations with Intelligent Automation

Sorting through and responding to operational alerts is just one area of IT monitoring and management that increasingly requires some level of automation. The combination of IT infrastructure complexity and distribution with the need for constant IT availability and speed have made many manual processes impractical or unfeasible.

Traditionally, some manual tasks have been automated simply by having monitoring systems recognize known operational conditions or deviations from baselines and respond with pre-programmed actions. Increasingly, however, automation is being supplemented and extended with AIOps – artificial intelligence for IT operations.

AIOps solutions draw from established best practices, normal operation parameters, and their interdependencies, as well as from machine learning algorithms and the models these algorithms create of existing infrastructure elements. The example cited earlier of a system understanding the anomalous context of a server's 80% capacity level could be one form of this intelligence. Broadly speaking, the functions delivered by AIOps can include everything from infrastructure mapping and reporting to automated incident identification and response.

A fundamental goal of AIOps is to make IT infrastructures as self-reliant and self-healing as possible. Achieving this goal ultimately requires that AIOps solutions identify and correct problems that even the IT managers may not have seen before or anticipated. AIOps must also be able to recognize and adapt to changes in IT components, configurations, and workloads with as little human intervention as possible.



Given the critical importance of getting IT operations right, organizations often want IT professionals in the decision-making loop for critical processes. For the foreseeable future, not many IT managers will be willing to rely entirely on machine intelligence to keep the IT lights on and shining brightly.

As such, the most useful and appreciated AIOps solution will let IT departments automate tasks at their own pace. IT managers can then expand the reach of AIOps-driven automation as they gradually gain confidence and trust in the capabilities and reliability of these sophisticated solutions.

Netreo: Full-stack Monitoring and Management

The concept of digital transformation has been a hot topic for several years and continues to be a core organizing principle for many organizations. However, while most of the world has already transformed to a near-universal digital reality, there are still manual and analog processes to digitize, plus a steady stream of new technologies to exploit.

Netreo, founded in 2000 and for the past four years one of the Inc. 5000's fastest-growing companies, has built a full-stack IT monitoring and management solution in use daily by thousands of private and public entities to oversee millions of IT and communications assets. The company has also developed a sophisticated AIOps product – AIOps: Autopilot – to complement its core solution.

As shown in Figure 1, The Netreo Professional Platform provides a full-stack, data center to cloud to edge monitoring and management capability. This agentless solution uses standard protocols and APIs to monitor everything from server and storage platforms to network equipment and traffic to cloud environments and application user experience. The platform provides a wide range of out-of-the-box integrations with hundreds of diverse IT devices and platforms and delivers needed information to IT executives, engineers, and operations professionals.

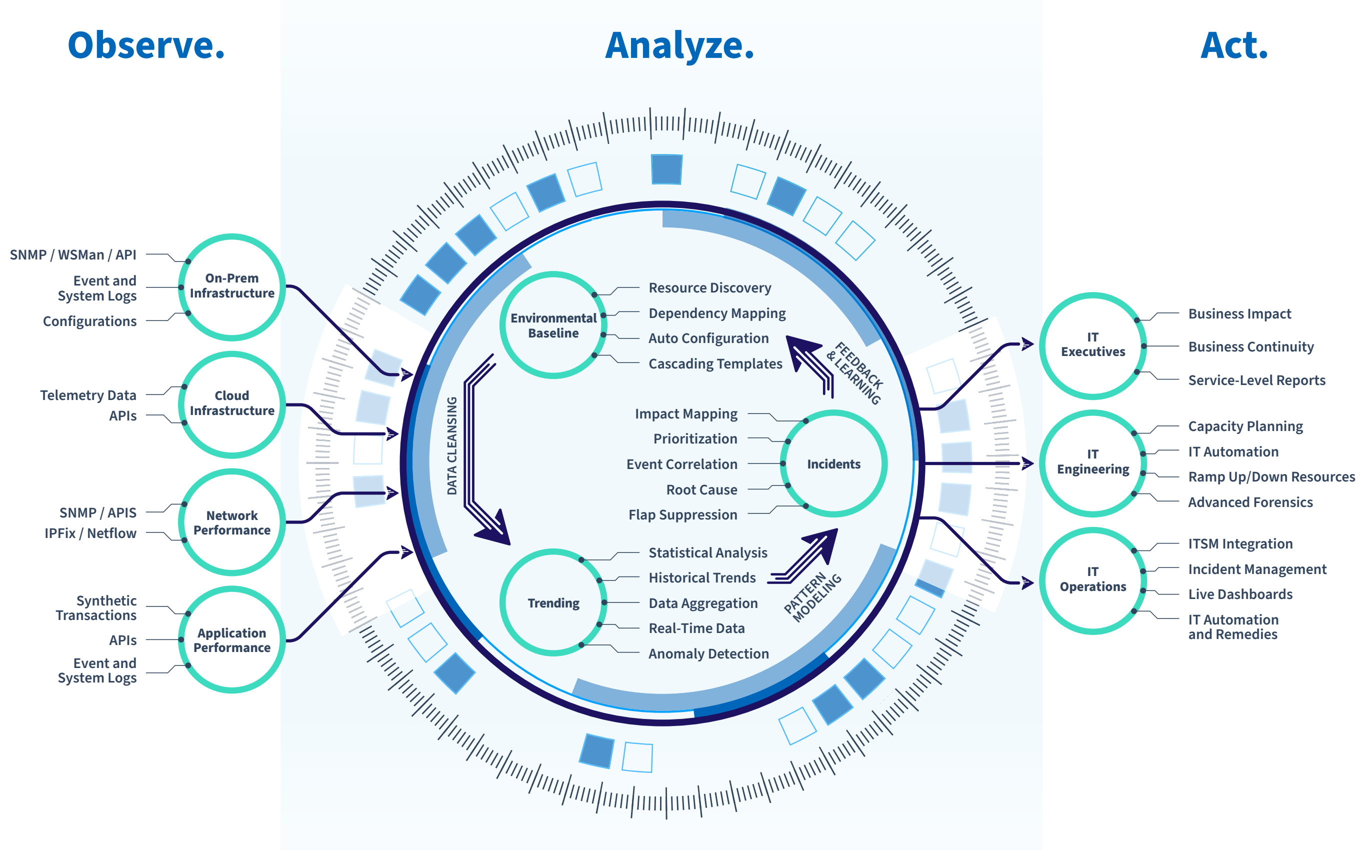


Figure 1. The Netreo Professional Platform – A Comprehensive Monitoring and Management Solution

Among its capabilities, the Netreo Professional Platform provides **intelligent alerts** of hardware and application failures or issues, automates a wide range of infrastructure monitoring and management activities, and creates a foundational single-source-of-truth database shared by the broad array of infrastructure elements from which it collects and analyzes data.

The platform's functionality spans everything from mobile device access to the platform's UI to network traffic analysis. Also – via the acquisition and integration of cloud-monitoring specialist CloudMonix and its technologies – the **Netreo Cloud** provides deep-dive visibility into public, private, and hybrid cloud environments.

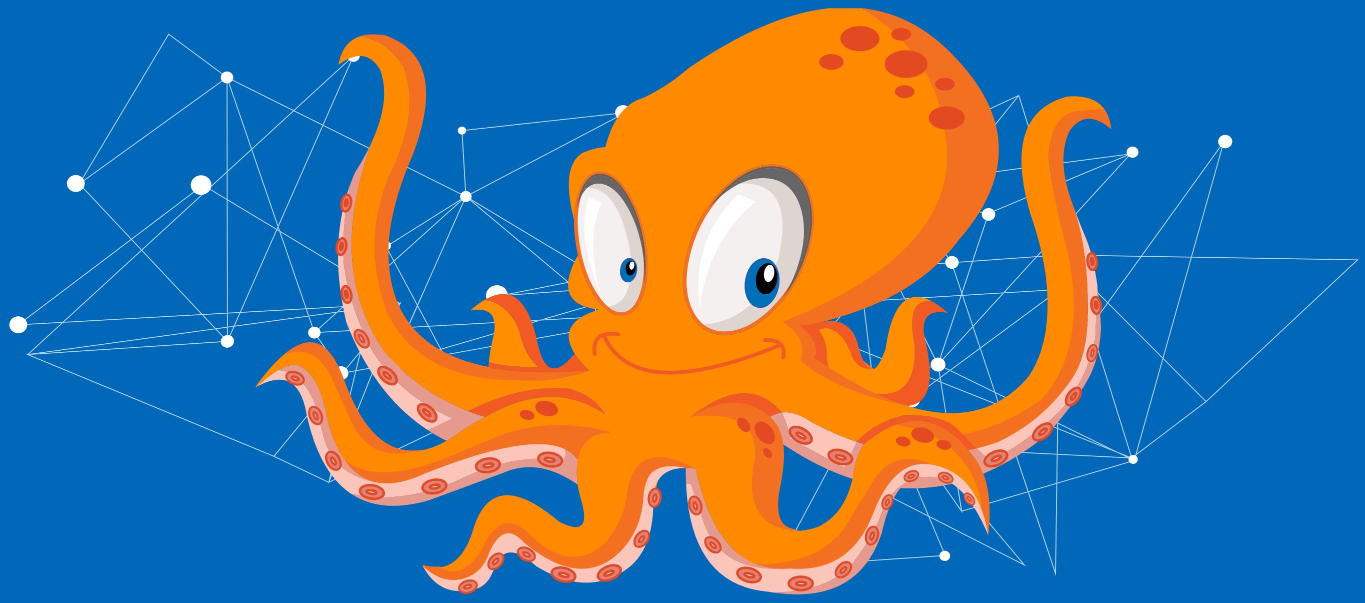
Beyond its core platform, Netreo offers two optional solutions. One, **Netreo Microsoft 365 Insight**, delivers targeted observation, analysis, and response capabilities to the many organizations that have deployed Microsoft 365. Among its capabilities, the Netreo solution provides digital experience metrics of remote users' experiences with Microsoft 365 elements. By delivering complete visibility into the Microsoft 365 productivity suite, Netreo Microsoft 365 Insight helps organizations track and fine-tune the suite's supporting infrastructure elements, monitor suite usage and licensing data, flag any operational problems, and ensure optimal Microsoft 365 performance.

The second optional solution, **Netreo AIOps: Autopilot**, helps make network management and monitoring self-tuning and self-healing. The solution uses a combination of best practice models and machine learning technology to scan deployment and data configurations, identify ways to optimize operations, and automate a variety of management tasks – all at the discretion of IT managers. For example, AIOps: Autopilot can recognize that improperly set thresholds are resulting in too many false alerts, guide IT managers about how best to recalibrate those thresholds or recalibrate thresholds automatically.

All told, the Netreo portfolio gives IT managers the tools and capabilities required to keep the digital heartbeat of their organizations healthy and beating strong.

For further information about how Netreo can help you meet the challenges of full-stack, end-to-end IT infrastructure management,

VISIT NETREO'S HOMEPAGE



Netreo's award-winning full-stack IT management and AIOps products empower customers with real-time information on their cloud, on-premises, and hybrid networks, applications, and devices — so they can provide amazing internal and external customer experiences from their digital environments and focus more on innovation. Netreo, used worldwide by thousands of private and public entities, monitors tens of millions of assets and devices per day. Netreo is one of Inc. 5000's fastest-growing companies.