

# Site24x7 RFP

## About us

ManageEngine Site24x7 is an AI-powered observability platform for DevOps and IT operations. The cloud-based platform's broad capabilities help predict, analyze, and troubleshoot problems with end-user experience, applications, microservices, servers, containers, multi-cloud, and network infrastructure, all from a single console. For more information about Site24x7, please visit [www.site24x7.com/](http://www.site24x7.com/)

S.No.	Solution Support	Specification (Yes/No)	Remarks
<b>A</b>	<b>General</b>		
	Drilled-down monitoring of individual resources for a detailed view		
	Integration or data Collection supported methods (e.g. API, events, SNMP v3 polling, streaming, logs, OS forensics, WMI, syslogs, SSH, and custom).		
	Support with own tool, native agent, third-party agent (e.g. Fluentd), or cloud-native Agent (e.g. CloudWatch) for in-depth metrics discovery and monitoring		
	In-built cloud storage for SaaS monitoring		
	On-the-go monitoring with Android/iOS mobile apps		
	Periodic online/on-site training and certification courses with regular product updates via newsletters		
	Thriving user community with seminars and user conferences held worldwide		
	Optional on-site visits and onboarding assistance with product training		
	24x7 mail and call support		
	Codify knowledge and best practices to make workflow executable (Tech documentation, troubleshooting guides, explanatory videos)		
	Multi-tenancy and role-based access control (RBAC) for different tenants, groups, accounts, or resource hierarchies		
	Offerings for managed service providers (MSP) and cloud service providers (CSPs), and Business Units (BU) offerings to organize monitoring among subteams		
<b>B</b>	<b>Architecture</b>		
	Simple to configure with no support for day-to-day operation (Ease of management)		
	Support for agent-based (in case required for specific instances) and agentless monitoring with a probe-central architecture for distributed/multi-site monitoring		
	Monitoring support for IaaS, SaaS, physical, virtual, and hybrid platforms		
	Out-of-box deployment without customer-specific developments		
	Easily scalable for ideal enterprise infrastructure		
	Integrated solution for end-user experience, infrastructure, and application monitoring		

	Integration with third-party applications at the user-interface layer through APIs		
<b>C</b>	<b>Detailed Monitoring Capabilities</b>		
<b>Ca</b>	<b>End-user experience monitoring</b>		
	Monitor the availability and performance of websites and FQDNs		
	Identify ISP latencies		
	Monitor the business activities and capture in which step a problem may occur both synthetically and in real-time		
	Provision to record and play user interactions at different steps		
	Website hostname or IP address checks against DNS-based blocklists		
	Periodic SSL/TSL certificate and domain expiry checks		
	Periodically check the website on the Web Risk list for malware, untrusted software, and social engineering tactics		
	Availability checks for website components like DNS server, POP server, mail delivery server, WebSocket, FTP server, and others		
<b>Cb</b>	<b>Infrastructure</b>		
	Able to discover full-stack IaaS and PaaS (Compute, app, Kubernetes, cloud networking, cloud IAM, Cloud audit, Cloud logging, and serverless functions and services) and support auto-scale Up/Down discovery/termination for monitoring		
	Automated discovery and mapping of an application and its infrastructure components (including cloud services)		
	Automatically map and track infrastructure, app, and service dependencies to understand the business impact		
	Track the health, performance, and uptime of multi-cloud/hybrid-cloud resources and the application workloads		
	Able to monitor container health and resource utilization metrics for clusters, nodes, and namespaces at service-level and pod-level		
	Proactive monitoring to fix problems before they happen		
	Configuration management database (CMDB) accuracy with real-time sync of monitored environments		
	Automate diagnoses with Runbooks, isolate performance issues at the network layer or application level, and accelerate Root Cause Diagnoses (RCD)		
	Multi-vendor support for physical and virtual networks and security devices deployed in DC or private/public cloud for monitoring		
	Provision to build monitoring/workbook via API, SSH/CLI, REST, JMX, and other data collection methods to automate security assessments/MBSS and daily checklists, and proactively guard against non-compliance.		
	Prioritize work based on business impact with a fast drill down to the root cause		
	Secure, reliable, available, and scalable for future growth and new cutting-edge technology upgrades (Multi-cloud/SDN/NFV/SD-WAN/IoT/Edge computing/SASE)		
	Able to capture detailed inventory for cloud-native resources as well as NVAs (marketplace BYOL virtual appliances) and physical devices		

	Automated change management to reduce human error in network changes, push changes with one click, and validate changes visually		
	Visual network management with end-to-end visibility and management		
	Topological visibility for complex hybrid networks		
	Source-to-destination path mapping and analysis with telemetry plotting with hop-by-hop latency and other critical telemetry measurements		
	Intelligent traffic flow analytics to analyze network traffic flows based on source, destination, ports, and protocols (NetFlow, sFlow, J-Flow, cFlow, AppStream, IPFIX, NetStream, and AppFlow )		
	Network baseline configuration and changes made over time		
	Configuration backup and life cycle management to revert to the previous configurations in a device in case of security issues		
	Support to monitor the cloud services and deployments across multi-cloud		
	Software-defined networking monitoring		
	Monitor and understand cloud spending patterns. Visualize costs in your cloud billing, allocate cloud budgets, utilize tags, and create business units for cloud costs to track the cost optimization journey		
<b>Cc</b>	<b>Observability</b>		
	Visualize application flows and interconnects dynamically		
	Provide Apdex scores to analyze the health and performance of applications		
	Performance analysis for applications written in Java, .Net, Python, PHP, Node.js, and Ruby on Rails		
	Observation of an application's complete transactional behavior		
	Monitoring of applications delivered via browser, mobile app, and API		
	Identification and analysis of application performance problems and their impact on business outcomes		
	The ability to perform interactive exploration and analysis of multiple telemetry types (metrics, traces, and logs) to identify and explain the causes of unexpected events, exceptions, and anomalies		
	The ability to track individual transaction traces across applications, microservices, and distributed architecture		
	Locate application workflow anomalies by mapping application dependencies		
	Record significant events like build deployments, product updates, feature enhancements, and infrastructure upgrades		
	Track the performance of mobile applications, including those deployed on the cloud, with device-wise and geography-wise usage stats		
	Mobile application crash analysis with details like the percentage of crashes over a time period, corresponding devices, and the affected users		
	Log analytics for troubleshooting applications, cloud-native services, compute and serverless infrastructure, and Iaas/PaaS		
	Log ingestion via log shippers like Logstash and Fluentd		
	Correlate application behavior with hosted infrastructure by analyzing logs from both application and infrastructure		
	Query-able log data with results displayed as charts for easy analysis		

	Dashboards for analyzed log results		
	Alerting based on log search results		
<b>D</b>	<b>Dashboards and Reporting Capabilities</b>		
	Creation of customized dashboards for NOC and operations teams with the ability to share		
	Define SLAs based on different metrics like availability and performance		
	Current and historical out-of-the-box reports for various statistics monitored		
	Ability to create the current and historical reports via the web console		
	Allow advanced customization by providing options to enter custom queries to extract data from the database directly		
	Options to export reports in multiple formats such as PDF, HTML, and CSV		
	Integration with other IT analytics solution for detailed analytics		
	Integration with other IT analytics solutions for detailed analytics		
<b>E</b>	<b>Alerting Capabilities</b>		
	Support alerts, events, notifications, logs, and trap collection		
	Generate alerts via Email, SMS, voice call, and push notifications on mobile apps		
	Alert Management without any manual intervention. Auto-resolving problematic resources using in-built, out-of-the-box, or customizable automation		
	Create and enrich incidents with real-time diagnostic information and automation for raising incident tickets using ITSM, collaboration, workflow, and analytics tools		
	Pre-built rules (default settings) for threshold settings and alarming rules		
	Ways to manually define monitoring thresholds and alarming rules		
	Provisions to define a mixture of alerting methods within a single rule		
	Configurable escalation levels		
	Allow configuring a logic for alerting		
	Configure different severity levels for alerts		
	Create, update, and delete rules per monitor or group of monitors		
	Dynamic, AI-based threshold configurations		
<b>F</b>	<b>AIOps Capabilities</b>		
	AI/ML-powered anomaly detection and forecasting engine for potential issues. Ability to identify and detect the root cause of a problem quickly with AI/ML engine and resolve issues before end users/applications are affected		
	Predict and forecast performance metrics/KPIs based on historical observations, behavioral data, and AI/ML		
	Automatically detect weird and anomalous patterns and shapes of performance data		
	Automatically correlate events and anomalies to reduce noise and identify service-impacting issues		

	Visualize performance hotspots and anomalies in real-time		
	Automation for troubleshooting and fixing issues automatically for faster MTTR		
	Automate operational data workflows for performance insights		
	Automatically capture real-time diagnostic data at the time an event occurs.		
	Automate CI lifecycle, configuration, change, problem, and compliance management		
	The ability for preventive automation using adaptive monitoring, Network intent-based automation for well-known diagnosis, self-service Automation, interactive automation, and collaborative automation.		
	Monitor and automate unique or custom technologies, processes, and workflows at our own pace.		
	Automate diagnoses with Runbooks, isolate performance issues at the network layer or application layer and accelerate root Cause diagnoses		
	Automated change management to reduce human error in network changes		
	Dynamic thresholds that are AI-based based on behavioral analysis to alert of unexpected changes proactively		
	NLP-based communication medium for clarification of monitoring queries		
<b>G</b>	<b>Security</b>		
	Data encryption with data residence within regional boundaries. Redundant data centers in common regions like the EU, the US, China, Japan, Australia, and India		
	User authentication capabilities like SSO, MFA, and biometrics		
	Role-based access control to restrict users from accessing critical features		