



Advanced synthetic monitoring strategies with Site24x7:

Simulating real user journeys

What are we going to cover?

Introduction	3
How organizations benefit from synthetic monitoring	4
Core capabilities of Site24x7's synthetic monitoring.....	7
Smart alerting and AIOps features.....	12
Alert management in synthetic monitoring	14
Conclusion.....	15



Introduction

Today's users expect flawless digital experiences, with even brief slowdowns potentially damaging brand perception and revenue. PwC's 2024 CX report shows that one-third of customers disengage after a single bad interaction, and over 90% leave after repeated disruptions.

Meeting these expectations requires more than reactive monitoring. Traditional tools often miss issues in login flows, DNS records, or third-party services because they rely on real user traffic. Synthetic monitoring addresses these gaps by proactively simulating user journeys from global locations, detecting failures before they affect customers.

In the following sections, we'll explore how organizations use Site24x7's synthetic monitoring to detect issues early, improve operational efficiency, and deliver reliable digital experiences at scale.



How organizations benefit from synthetic monitoring

To understand how synthetic monitoring enables early detection and faster response, it's best to look at how companies are leveraging Site24x7 to maintain uptime and deliver consistent digital experiences at scale.

The examples below highlight how teams across industries are already using Site24x7's synthetic monitoring.

Publicis Sapient: Proactive monitoring across client environments

Publicis Sapient, a global digital consultancy firm, manages complex environments for over 25 managed service clients. It needed a scalable solution that offered full-stack observability with strict client-level data segregation. Site24x7 met this requirement while enabling the company to upgrade from basic uptime checks to robust synthetic transaction monitoring.

Using Site24x7's browser-based recorder, the team simulated real user workflows, such as login and checkout journeys, across key digital assets. These synthetic tests helped detect issues in payment gateways, SSO sequences, and third-party integrations before they impacted users.

As a result, Publicis Sapient significantly reduced mean time to detect (MTTD) and experienced fewer client-reported incidents.

Their operations center also adopted Site24x7's NOC dashboard, allowing for real-time prioritization of issues. For clients migrating from open-source solutions, the built-in infrastructure and network monitoring also helped eliminate cost overruns and blind spots.

In the end, the Site24x7 platform became central to Publicis Sapient's promise of always-on reliability.

Telefónica España: Unified visibility across teams

Telefónica España, one of the largest telecom providers in Europe, turned to Site24x7 to overcome limitations in its existing monitoring tools. The company sought a comprehensive platform to unify its internal systems monitoring with synthetic tests for public-facing services.

After implementing Site24x7, Telefónica structured its monitoring into two distinct groups: one for internal applications and another for production systems. This segmentation allowed for tighter collaboration across teams and faster triage of emerging issues. Synthetic checks exposed DNS latency and region-specific login failures early, reducing mean time to repair (MTTR) and preserving user satisfaction.

The platform's flexibility also allowed Telefónica to adapt its monitoring strategies based on application criticality, ensuring both high-frequency testing for sensitive systems and broad coverage for supporting services.

IIFL: Financial services resilience through synthetic insights

IIFL (India Infoline), one of India's leading financial service providers, operates a high-stakes digital trading environment where downtime can directly impact revenue. To meet strict SLA requirements and customer expectations, IIFL implemented Site24x7's synthetic monitoring suite.

The team configured transaction monitors to simulate login flows, session handling, and API responsiveness across its multi-cloud infrastructure. These proactive checks helped IIFL identify slowdowns and errors before traders encountered them, significantly improving uptime adherence.

Site24x7's consolidated dashboard also enabled visibility across both on-premises and cloud environments, reducing tool sprawl and improving response coordination. Over time, IIFL achieved a 20% reduction in monitoring-related operational costs while boosting reliability and control over its digital assets.

Although the above three companies operate in different industries, they share a common goal: identifying issues before users are affected. Their use of synthetic monitoring goes beyond simple prevention. It plays a strategic role in reducing downtime, maintaining trust, and delivering consistent digital performance at scale.

These use cases demonstrate that by simulating user journeys and proactively detecting faults, teams can respond faster, protect brand reputation, and improve customer retention.

Core capabilities of Site24x7's synthetic monitoring

While the scenarios discussed in the previous section varied, Site24x7's comprehensive synthetic monitoring suite served as the technical foundation for all three. In this section, we'll break down the platform's core capabilities—from simulating full browser transactions to detecting anomalies through AI-powered baselining.



Wide range of synthetic monitors

Site24x7 offers a comprehensive set of synthetic monitors that simulate interactions across all major digital touchpoints:



HTTP/HTTPS uptime checks:

Perform continuous health checks on endpoints to validate availability, status codes, response times, and SSL certificate validity; ideal for detecting outages or latency spikes across CDNs or edge networks.



Webpage speed (browser) monitors:

Use real browser engines (Chrome/Firefox) to analyze page load performance, resource-level timings, and DOM interactive and contentful paint metrics; you also get support for performance baselining via web vitals.



Browser-based web transaction monitors:

Simulate multi-step workflows like login, search, form submission, and checkout using a recorder or custom Selenium scripts; this is useful for validating frontend logic and session-dependent flows under real conditions.



Synthetic mobile application monitoring:

Reproduce user interactions on mobile apps using step-by-step flows; track API responsiveness, screen load times, and interaction latency across platforms (Android) and device emulators; schedule tests across geographies to detect regional latency or mobile CDN issues.



API monitors (REST, SOAP, gRPC):

Test single and chained API endpoints for latency, authentication (OAuth, headers), payload schema, and error handling; enjoy support for assertions and variable passing for deeper functional validation of business logic.



SaaS synthetics:

Monitor the availability and performance of third-party SaaS applications like Salesforce, Microsoft 365, and Zoom to catch upstream failures.



Internet performance monitoring (DNS, port, ping, SMTP, ISP latency):

Diagnose issues in the network stack by validating domain resolution, port accessibility, mail server uptime, network reachability, and last-mile ISP

Multi-location and device-based testing

Modern applications must work consistently across fragmented digital ecosystems. Without synthetic testing that accounts for both location and device variability, teams risk blind spots that only surface when users complain.

Site24x7's approach ensures performance validation under diverse real-world conditions, whether a user is accessing your service from rural areas or from a Chrome browser on a high-speed connection in New York.

Testing from 130+ global locations

Site24x7 synthetic monitors can be executed from over 130 global test locations worldwide. These nodes span major cities, ISP regions, and cloud providers to reflect real-world user traffic. Teams can choose to run tests from:



Public nodes:

Managed by Site24x7, these are ideal for testing publicly accessible applications and APIs across geographies.



Private nodes:

Deployed behind the firewall within enterprise environments, these test internal apps, intranet portals, or geo-restricted services.

This dual-node approach ensures organizations can monitor both external user-facing systems and internal enterprise applications with the same level of precision.

Additionally, monitoring from centralized locations often misses location-specific issues. Multi-location testing addresses this by uncovering problems such as:

- DNS resolution failures due to misconfigured records that only affect certain resolvers
- SSL handshake issues arising from incomplete certificate chains not accepted in specific regions
- CDN propagation delays, where newly deployed content takes time to reach edge nodes
- ISP peering or routing issues, which cause elevated latency or packet loss for users on certain providers

By validating performance from the same regions as your end users, Site24x7 helps localize the root cause of user-facing anomalies.

Browser & mobile emulation

User experiences vary significantly depending on the devices and browsers being used. Site24x7 enables synthetic monitors to emulate traffic from various user agents, including:

-  Desktop and mobile viewports
-  OS-specific environments (e.g., Windows, macOS, Android, iOS)
-  Browser engines (e.g., Chrome, Firefox, Edge)

For mobile applications, Site24x7 supports synthetic monitors that mimic user behavior on native apps. Teams can define step-by-step flows (e.g., login, swipe, tap, API fetch) across:

-  Android platforms
-  Multiple device emulators
-  Geo-specific mobile networks or regions

This device-level simulation helps teams detect issues such as:

-  Layout shifts or responsive design bugs on smaller screens
-  JavaScript errors tied to specific browser versions
-  Inconsistent rendering of web components across engines

Teams can also validate the performance at the API, UI, and network layers, catching latency spikes, failed interactions, or app crashes before real users are impacted.

Smart alerting and AIOps features

Managing alert fatigue is one of the biggest challenges in synthetic monitoring. Site24x7 addresses this with alerting and anomaly detection, driven by machine learning (ML), to reduce noise while maintaining accuracy.

Adaptive thresholds & intelligent baselines

Historical performance data, such as page load times and web vitals, is continuously analyzed with ML models to create dynamic baselines. These baselines adjust automatically to seasonal usage patterns and load variations. When deviations occur, Site24x7 flags them as anomalies instead of triggering static threshold breaches, cutting down on false positives.

Teams can also define granular thresholds by location, time window, or user group. For example, acceptable response times in low-traffic overnight hours can be set differently from daytime business periods, ensuring alerts are always relevant to context.



Predictive insights & AI-driven root cause detection

At the center of Site24x7's AIOps layer is Zia, the AI assistant that enables natural language queries on monitoring data. Teams can ask questions like “What was the average load time in Singapore last week?” or “When did login transactions start failing?” to receive instant insights.

Zia not only correlates recurring issues across monitors but also forecasts potential SLA breaches using historical patterns. This allows teams to take corrective action before users are impacted, making synthetic monitoring proactive rather than reactive.

Alert management in synthetic monitoring

Site24x7's synthetic monitoring suite is equipped with an intelligent alerting system designed to surface only actionable incidents while suppressing redundant or low-priority noise. At its core is adaptive thresholding powered by the ML capabilities for anomaly detection discussed in the previous section.

Smarter thresholds & noise reduction

To avoid alert storms during correlated failures, Site24x7 groups related synthetic alerts into a single incident. If an upstream API fails, for instance, resulting transaction failures across multiple monitors are bundled and flagged with the likely root cause.

Dependency-aware suppression ensures that failures cascading from shared infrastructure, such as DNS or authentication services, are not unnecessarily repeated across dependent monitors.

Precision routing & integrated workflows

Alerts can be routed with tags that align with monitor type, geography, or service ownership. Maintenance windows and suppression policies further reduce noise during planned downtime.

Each alert includes complete diagnostic context, such as failed steps, HTTP response, timing details, and test location, making them immediately actionable.

Site24x7 integrates with popular collaboration and incident management tools, including PagerDuty, Opsgenie, ServiceNow, Jira, Microsoft Teams, and Slack. Escalation rules and routing paths ensure alerts reach the right team without overwhelming them.

Deep diagnostics & APM integration

Beyond alerting, Site24x7 enhances RCA with both network and application-level diagnostics. For HTTP response code errors, teams gain instant access to traceroute, ping analysis, DNS reports, and MTR-based network paths to identify connectivity or latency problems.

Synthetic monitors are also integrated with Site24x7's APM suite. When a synthetic test fails, it is automatically linked to an APM trace, showing the exact cause of the issue, such as an SQL query timeout, Java exception, or third-party dependency error. This combination of synthetic checks with full-stack APM traces provides a complete view from symptom to root cause, enabling faster and more precise resolution.

Conclusion

Ensuring digital reliability today means more than just catching incidents—companies must anticipate them. Site24x7's synthetic monitoring suite helps teams simulate real user journeys, detect anomalies early, and maintain end-to-end visibility across distributed systems.

Site24x7 offers extensive synthetic monitoring, covering HTTP checks, multi-step browser flows, mobile apps, API chains, SaaS, and infrastructure. It simulates user behavior globally across devices, while AIOps features like adaptive thresholds, anomaly detection, and correlated alerts ensure precise, noise-free alerts and faster issue resolution.

All of this empowers SREs, observability engineers, and platform teams with better uptime control, SLA assurance, and incident prevention, providing proactive insights for performance at scale. To learn more about Site24x7's capabilities for your environment, explore our extensive documentation, start a free trial, or sign up for a customized demo for your specific use case.

About ManageEngine Site24x7

ManageEngine Site24x7 helps teams monitor Kubernetes clusters effortlessly with full-stack observability that combines metrics, logs, and traces into one cohesive view. With intelligent alerting, auto-discovery, and built-in dashboards, Site24x7's Kubernetes monitoring enables engineering and DevOps teams to detect, troubleshoot, and resolve issues faster across dynamic container environments.

[Get Quote](#)[Request Demo](#)