Beyond Monitoring: The Power of Comprehensive Observability

How Automation, AI, and Real-Time Data are Transforming IT Operations

As IT environments grow in complexity, the need for comprehensive visibility into operations has never been more critical. Businesses need complete visibility into their IT operations to stay ahead of performance issues, security threats, and unexpected downtime. Traditional monitoring tools - while useful - often fall short, providing fragmented data that leaves IT teams reacting to problems instead of preventing them.

Many organizations have taken a platform-centric approach to observability. They monitor network consoles, security consoles, and other tools to try to understand how things are running today and, hopefully, gain predictive insight into what may happen in the future.

This approach has led to frustration among IT leaders, because despite substantial investments in observability, much of operations remains reactive instead of proactive.

Seamless IT operations hinge on the ability to collect data that can provide insight into operations and present that data to the proper stakeholders, who can then ask questions of the data to make better decisions about their IT environment. Stakeholders can include IT and executive decision makers, operations teams, and digital Interfaces such as AI and automation tools.

True comprehensive IT visibility and observability goes beyond simple monitoring to provide a complete, real-time picture of an organization's IT health. It enables IT teams to move from reactive troubleshooting to proactive prevention, enabling better decision-making, stronger security, and a reliable user experience.

Core Components of Comprehensive Observability

A more productive approach is data-centric rather than platform-centric. By collecting, aggregating, and analyzing the right observability data, organizations can see a more holistic picture of their environment, which enables them to make better decisions. More specifically, observability data helps IT teams better understand:

- User experience
- Application performance
- Capacity, utilization, and availability
- Security and risk — both latent and ongoing
- Problem root cause

Logs, Metrics, and Traces

There are three types of data to collect and aggregate for comprehensive observability:

- Logs
- Metrics
- Traces

For example, if CPU utilization spikes to 95% and starts to erode the user experience, you can see what's driving the spike, such as a superfluous process running periodically. Maybe that process was started by an unauthorized intruder. Or perhaps it's tied to an actual process that simply needs the extra capacity periodically to keep up. Correlated observability data can help you determine whether or not the spike is a real issue that needs investigating.

Logs, Metrics, and Traces

Logs document systems activities such as a user logging into an environment or launching an application. Logs can also include how an application is being used and errors generated.

Traces follow a workflow as it moves through the network and documents communication between components, showing who communicated and what was communicated. For instance, trace enables you to see the flow of someone logging into your website and using an application to order a product, triggering the application to access your ERP system to check inventory.

Metrics are the common data center measurements and include things like CPU utilization, memory utilization, and thresholds. Metrics are measurements of what's going on in any individual component or system subcomponent. They can also reflect larger concepts such as response time.

Logs, metrics, and traces aren't new. Each of these, on their own, are useful, but they only tell part of the story. What's changing is the ability to leverage the right data to triangulate events to see the broader context for what's happening in the environment. By layering in and correlating more information, organizations can get more value from observability. This is a classic example of turning data into actionable information - action that can be taken by automations or people.

Benefits of True Observability

One of the main benefits of comprehensive IT observability is that it enables IT operations teams to shift from reactive to proactive. This frees up IT teams to go beyond basic system maintenance and explore new business opportunities through technology. Advantages that organizations can experience when IT teams take a proactive approach include:

- Improved and more reliable user experience
- Improved security through enhanced visibility
- Improved IT availability and reliability
- Improved developer experience and productivity
- Faster incident detection and resolution
- Reduced downtime

There are also several benefits for consumers of observability data, including the ability to:

- Respond quickly to events
- Resolve known issues without reaching out to IT support
- Resolve security issues quickly
- Apply analytics or AI to predict or identify issues

For example, in a hypothetical environment, it may be standard procedure to reboot a server if it reaches 95% memory utilization. To automate this, you can monitor for 95% memory utilization and trigger a script that handles the reboot process, including redirecting traffic during the reboot and validating that it was successful. The script can even automatically open and close a ticket in the service management system, eliminating another manual step in the process.

Or, on the security side, unusual disk activity resembling encryption could trigger an automatic response to isolate the affected server by shutting down all network connections. This prevents threat actors from potentially pivoting to other devices.

The Role of Automation in Observability

If you're not living in a world where automation is essential, it won't be long before its benefits will become more compelling. In the modern IT environment, there's simply too much to accomplish and too much risk of error to rely on manual processes.

Automation Makes Observability More Powerful

Automation is essential to ensure that your observability platform is populated with current, accurate data and that data is delivered in a timely manner to its constituents.

Automation enables observability to be more powerful because it can enhance the ability to be more fully instrumented, and therefore, have a more comprehensive context to better identify what's driving anomalies in the IT environment.

Automation helps you build the observability environment by collecting observability data — logs, metrics, and traces — from observability endpoints, which oftentimes is done by an agent. This is difficult to do without automation.

Automate Data Normalization

A key challenge in developing comprehensive observability is pulling all the data together and normalizing it through transformations. This is a great use case for automation. For example, metrics pulled from switches are formatted differently from metrics pulled from storage arrays. So, your observability solution must be able to normalize data from different sources and enable you to select the data you really need because you most likely don't need all of it.

In addition, automation makes it much easier to present the data in a way that's relevant to the various stakeholders. This can be done through a business intelligence platform, a security information and event management (SIEM) system, or a GenAI platform that enables users to ask natural language questions of the data. As observability data consumers, automations can act on alert data to respond to an issue.

How Comprehensive Observability Enhances Security

Comprehensive observability creates a foundation for handling security tasks that organizations tend to struggle with. Given comprehensive observability data available for analysis, patterns can be revealed that would otherwise not be detected.

For example, log data on its own may not reveal anything of concern. The same with network traces. But by correlating the two, it could be revealed that there's traffic from an IP address outside the organization involved in malicious activity such as encrypting a volume.

Going Beyond Point Solutions

Almost all security solutions were developed to solve a specific problem. Still today, there isn't one security solution that rules them all. Over time, organizations have collected sets of tools to

Action Recommendations

At Evolving Solutions, our mission is to assist IT operational teams across various industries and sectors in making a pivotal shift. That shift involves transitioning from a reliance on traditional metrics to one of adopting a dynamic, process-oriented perspective. To navigate this transition and ensure that it aligns with the initial objectives, we propose a set of action items designed to enhance both business outcomes and end-user experiences.

Develop KPIs based on business outcomes and end user experience

Institute a workflow-focused monitoring approach

Create plans to seek insights into process performance, not just component performance

Organize cross functional teams and processes to enable the foundation of success

Adopt automation to accerate the return on investment

Leverage AI to enable IT Operations focus on business-critical issues first

solve specific problems but haven't developed a strategy or technical integrations to unify them. Comprehensive observability enables organizations to develop a unified strategy for security and performance monitoring using, in most cases, tools they already have. The result is the ability for multiple constituents to make good operational decisions based on trustworthy data.

AI and Observability: A Powerful Partnership

AI can make observability more powerful by leveraging logs, metrics, and traces for predictive analytics. AI also helps facilitate observability through thresholding and normalization. By understanding what normal behavior looks like, an AI tool can identify abnormal behavior and dynamically make adjustments — or not — depending on the context. For example, a CPU at 95% utilization can be cause for concern. But what if the spike only happens a couple times per week in response to a particular job? An AI can be trained to consider this normal activity, because you don't need to ramp up your data center or page another IT professional for known, transient spikes.

The Future of Observability

As IT environments grow more complex, organizations will need to move beyond traditional monitoring and embrace a more dynamic, intelligent, and automated approach to observability.

The next generation of security involves the ability to triangulate events in a more comprehensive way, which improves event discovery and remediation. It's also valuable for forensic research, because analysts can get a complete picture of how an event unfolded.

One major trend shaping the future is the increased role of AI and machine learning. AI-powered observability solutions will continue to improve anomaly detection, adaptive thresholding, and root cause analysis. Instead of IT teams manually sifting through data, AI will surface actionable insights in real time, helping organizations anticipate and resolve issues before they impact users.

Another key development is the rise of self-healing IT environments. By integrating observability with automation tools, organizations can enable auto-remediation, where systems detect, diagnose, and resolve issues without human intervention. This shift from reactive to proactive and predictive IT management will significantly reduce downtime and improve operational efficiency.

Additionally, the way organizations aggregate and search IT data will continue to evolve. While some will adopt a centralized data lake model, others will leverage federated search to analyze

Case Study

Client: Property, Life, and Casualty Insurance Company

CHALLENGE:

The organization was utilizing multiple observability tools and managing multiple vendor relationships that did not interact and share data, which was taking significant resource hours to address and created a lack of full-stack visibility within their environment.

HOW WE HELPED:

The Evolving Solutions team provided guidance and a roadmap for the organization to leverage an observability platform solution.

RESULTS:

The organization optimized resource time for more important tasks and freed-up resources as well as reduced tool spend and sprawl.

data across multiple sources without requiring full consolidation.

Finally, security observability will become a priority as organizations seek to enhance threat detection and incident response. With cyber threats growing more sophisticated, security teams will increasingly rely on observability data to correlate security events across infrastructure, applications, and endpoints, helping to detect hidden threats and automate rapid responses.

Position Your IT Environment for the Future

Comprehensive, unified observability is no longer just a "nice-to-have" for IT teams. It's a business imperative. As organizations become more reliant on complex, distributed digital infrastructures, gaining deep visibility into IT environments, predicting issues before they occur, and automating response actions will be essential for maintaining operational resilience.

As we look ahead, organizations that invest in a strong observability framework will be better positioned to navigate the challenges of modern IT management. Whether the goal is improving system reliability, enhancing security, or enabling self-healing IT environments, comprehensive observability provides the foundation for a more proactive, intelligent, and efficient IT strategy.

The question isn't whether organizations should adopt comprehensive observability - it's how quickly they can implement it to stay ahead in an increasingly complex digital world.

How Evolving Solutions Can Help

There are many steps in getting to unified observability and significant complexity on the journey. We start with your most pressing observability needs and work from there to develop a unified strategy and roadmap for success. Evolving Solutions is also here to help you create the necessary integrations and pull data together in a way that's comprehensively searchable and meaningful for stakeholders. And because IT systems generate a massive volume of log data, metrics, and traces, we help identify the data your observability platform needs to deliver meaningful insights and help you automate the normalization and transformation process. In addition, we can help you leverage tools you already have to create a unified observability framework.

Evolving Solutions is here to help your organization take an automated and AI-driven approach to observability. For nearly 30 years, Evolving Solutions has been helping business leaders take the next step in creating business value through technology. We have the skills, expertise, and experience to make your observability dreams a reality.

EVOLVING SOLUTIONS

We're here to help your organization take an automated and AI-driven approach to observability.

Let's Get to Work!