PULSEMETER

Techstrong Research

Infrastructure and Systems Management Calls for Unified, Predictive Solutions

by Guy Currier, Analyst, Futurum Group

SPONSORED BY Red Hat

Managing hybrid infrastructure—which in the modern IT shop includes public clouds; private clouds; on-premises and co-located systems and data centers; cross-platform virtualized Linux, other operating systems (OS), and container platforms; as well as numerous other resource automation platforms—has become a potentially massive task. The technologies are diverse. The highly dynamic nature of the modern application necessitates not just responsive but strategic management to ensure system health, security, and cost efficiency. And of course, the amount of data is ever-increasing.

The Challenges of Infrastructure Visibility, Security, and Efficiency

The foremost challenge is gaining comprehensive, but clear, end-to-end visibility across this fragmented technology stack. Monitoring tools too often operate in isolation, built for particular parts or capabilities of the infrastructure or application layer. However useful their insights may be, they are piecemeal.

The context-switching required to utilize multiple isolated monitoring tools hinders a shop's ability to correlate events and can easily limit the effectiveness of diagnoses and remediation.

Meanwhile, the dynamic runtime environment of containers and fluid application profiles driven today by rapid continuous integration / continuous deployment (CI/CD) pipelines requires system health monitoring that is both real-time and adaptive to avoid long production downtimes.

But beyond visibility, there are two critical management areas that are equally complex, if not more so. Resource optimization poses a significant challenge; the unpredictable demands of cloud and container environments, combined with the rigidity of on-premises infrastructure, can make it difficult to balance performance against investment and lead to overprovisioning, unnecessary costs, and ghost systems.

Key Takeaways

- Systems management is fragmented, with many organizations resorting to using multiple disparate tools to manage their hybrid cloud environments.
- Cross-platform system health is a challenge, requiring a combination of automated remediation, orchestrated response, and proactive monitoring.
- Automation prevails for both detecting and remediating security vulnerabilities, as well as applying system updates, but certainly has much room for development.
- Predictive analytics is perceived to be extremely valuable for identifying and addressing critical system issues.
- Traditional centralized management approaches—such as audits and internal controls—persist even as sophisticated infrastructure spending tools become widely available.

Current infrastructure automation often addresses isolated tasks with siloed solutions that can't capture the holistic complexity of modern, hybrid IT. A unified, predictive platform that provides comprehensive infrastructure oversight represents a transformative approach, so organizations can rapidly, consistently, and proactively manage, secure, and optimize their entire technological ecosystem at new levels of efficiency and intelligence.

Security across hybrid systems is also daunting, requiring consistent policy enforcement to catch issues early, rapid vulnerability response for the latest published Common Vulnerabilities and Exposures (CVE), and compliance management applied to sometimes wildly variant infrastructures and environments. Teams need to be able to accurately find and fix security events proactively *before* the next cybersecurity exploit.

Research Insights

In December 2024, Techstrong Research polled its community of infrastructure, systems management, and security readers and viewers to understand their experiences with, and what they need from, hybrid infrastructure systems management. The results revealed how many organizations are just beginning their journey toward automating infrastructure management, particularly in overall system health and performance with the important focus on security. Organizations are generally taking fragmented approaches, using that multitude of specialized tools that engender diagnosis and remediation challenges; they are essentially managing disparate infrastructure components separately, which makes full resource optimization a challenge.

Analyst View

Given the complexity and variety of modern infrastructure, it is no surprise that organizations are generally trying to make do with disconnected monitoring and management workflows. Roughly half of organizations use multiple separate tools to manage their infrastructure while only a third use single unified tools of one kind or another. This fragmentation creates significant challenges in obtaining an end-to-end view of the IT estate and enables full-context troubleshooting.

Meanwhile there is clear demand for advanced monitoring solutions that accurately detect issues and alert IT before users do. The vast majority of respondents to our survey, 85%, consider predictive analytics to be very or extremely valuable for identifying and prioritizing critical issues—most of these in the "extremely valuable" camp. There is a pressing need for proactive, intelligent monitoring tools that can cut through the noise and help infrastructure and security managers focus on only the meaningful insights—a need for the right teams to be notified at the right time with alerts that matter and few false positives.

About half of organizations use automation in incident response, either with a combination of automated remediation, orchestrated responses, and proactive monitoring (27%) or with automated workflows and playbooks (24%). Both of these areas can surely use improvement in the extent and capabilities of automation, but there are many organizations getting by without: a remarkable 19% still rely on manual processes. There is substantial room for improvement, especially in event-driven remediation that can cut down overall time to resolution.

Cost management is, of course, a critical optimization area in hybrid infrastructure management, and capacity planning is another area to target for improvement in order to get more predictability in cloud spending. A third of organizations use cloud cost optimization platforms and a third employ automated cost monitoring tools (with some using both)—but the number using arcane processes is great, rather than through the use of tools and technology that facilitate collaboration from a shared, holistic view. For example, the most common cost management method is simply the old-school centralized procurement process that does little to instill best practices for agile teams. Despite the considerable development and increased awareness of cloud cost control tools and technology, organizations seem to have a long way to go to modernize their approaches to IT financial management.

The security side of management shows a stronger level of automation. Three quarters of organizations surveyed use automated scanning as a key method to detect vulnerabilities and 33% rely on automated updates and patches. Human oversight remains a critical component of many security strategies, with a quarter to a third of organizations either adding it to automation, performing manual assessments, or relying on vendor notifications. We remain quite aware, however, of the degree to which security is

the perpetual wallflower, an afterthought, as for example how teams do not typically have visibility into transient dependencies in the technology stack or verified authenticity of early-stage development content—but are unaware of these gaps.

This poll nicely underscores the potential for critical transformation in infrastructure management, which must increasingly be in support of open, hybrid cloud. Organizations pervasively recognize the value of automated, predictive, and integrated solutions that unite monitoring, cost, and real-time security management across the estate. There is a clear imperative for continued investment in technologies that can provide holistic, intelligent oversight of complex hybrid cloud environments and ensure consistent delivery of value from an organization's infrastructure and the applications that run on it.

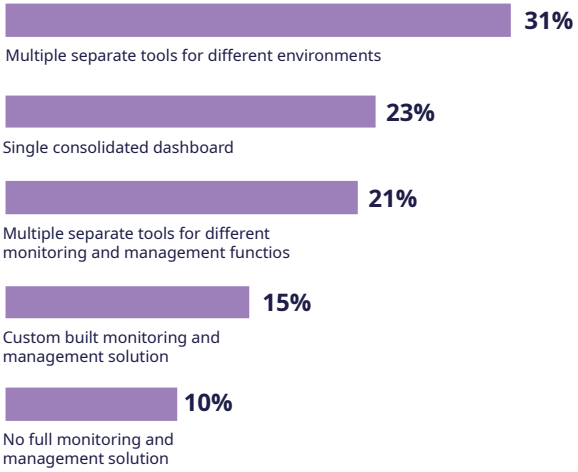
Recommendations

Platform engineers, IT service managers, and infrastructure managers should look closely at operations automation platforms that are unified and analytics-driven. As the infrastructure continues to evolve towards ever greater adaptivity and complexity while the urgency for openness and responsiveness remains, it can be a significant step forward to combine cross-resource visibility with clutter-clearing proactive guidance. This promises a welcome streamlining and simplification of monitoring, service resilience, and security management through automation.

Fragmentation—a prevalent issue in current hybrid setups—hinders visibility and response efficiency. Though hybrid management has been central to the construction and use of hybrid cloud from the beginning, it is only now reaching the maturity level of being able to span silos, provide end-to-end views, and enforce consistent policies and processes everywhere. Meanwhile, predictive analytics offers the ability to detect patterns, anticipate failures, and prioritize critical events before they escalate. It is not particularly new either, but the ability to feed it with the full range of cross-silo metrics and configurations is new. Organizations must, at the very least, look to bring disparate, manual processes to an end and incorporate more AI-driven, predictive, automated operations tools.

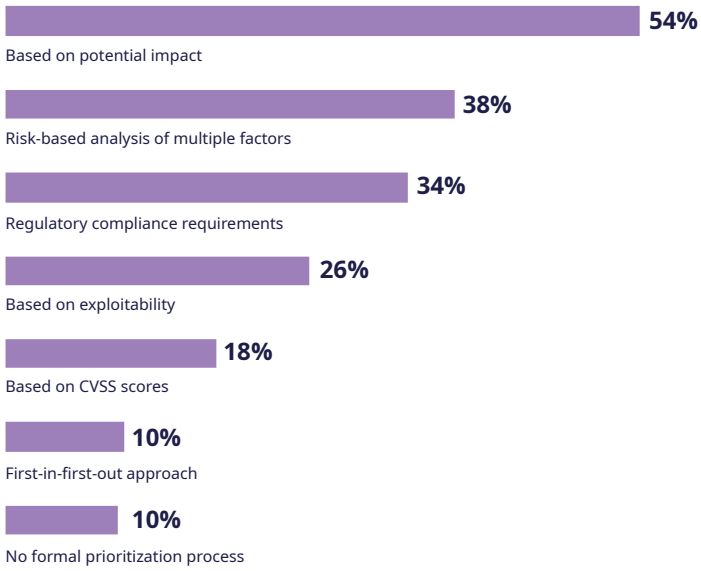
Research Results

Which of the following best describes how you currently monitor and manage systems across your hybrid cloud environment?



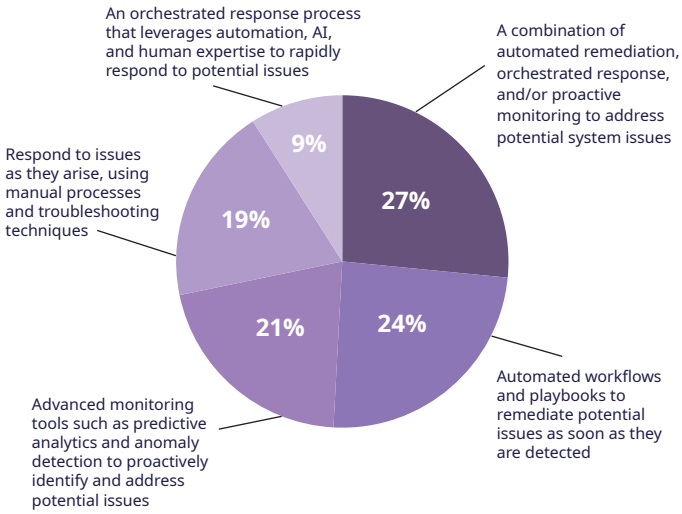
More than half (52%) of organizations use either multiple separate tools to monitor and manage their hybrid environments (31%)—or no tool at all (21%). Only about a third avoid a fragmented approach by using a single solution, either with a single dashboard (23%) or, for many of them (15%), with a custom-built solution they must maintain themselves.

What are the TWO most common ways you prioritize vulnerabilities to address within your environment?



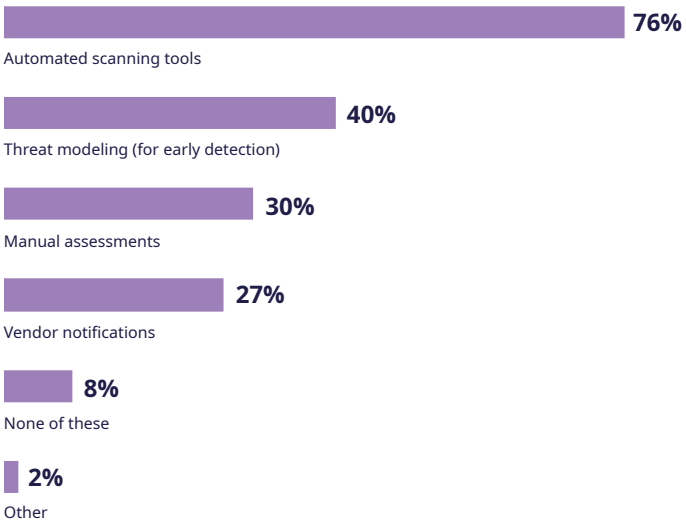
Almost all organizations use some form of formal vulnerability prioritization process; only 10% say they do not have one. For more than half of organizations (54%), a key prioritization method uses a measure of the vulnerability's potential impact. Only a little over a third (38%) say that the consideration of multiple factors is one of the two most common ways they assess the risk and priority of vulnerabilities, and a similarly small number (34%) use regulatory compliance requirements as a top factor in prioritization. Few organizations (19%) take advantage of CVSS, the Common Vulnerability Scoring System from the National Infrastructure Advisory Council, as a key vulnerability prioritization method.

How do you most typically address potential system issues BEFORE they impact your operations?



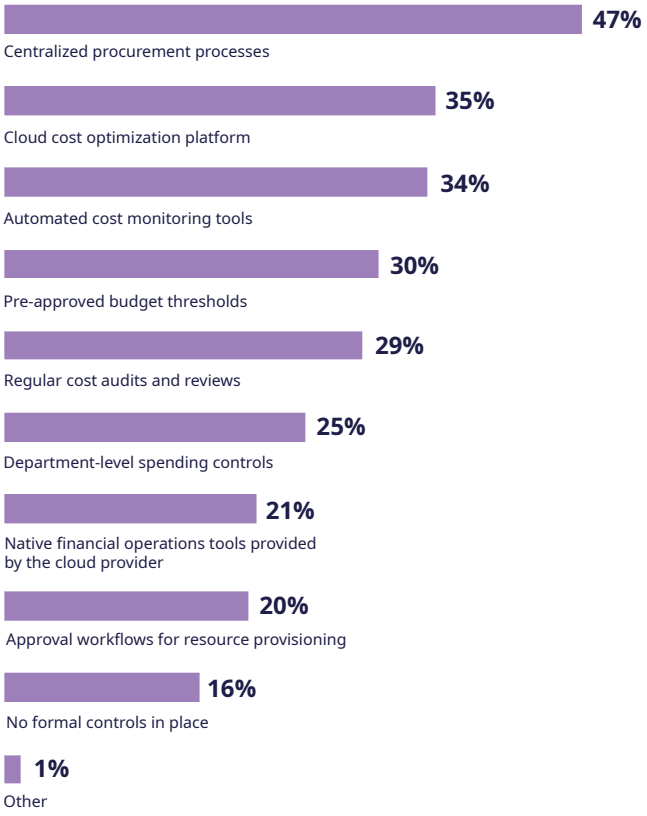
Despite this high demand for predictive analytics in systems management, however, about 7 in 10 organizations do not use it for this purpose. The most common approaches are a combination of automated remediation, orchestrated response, and/or proactive monitoring (27%), or high responsiveness to issues using automation and playbooks (24%), but a significant portion (19%) still relies on manual processes. Only about a fifth (21%) use predictive analytics and only 9% use AI (in combination with automation and human review).

Which methods do you rely on most to detect security vulnerabilities in your systems?



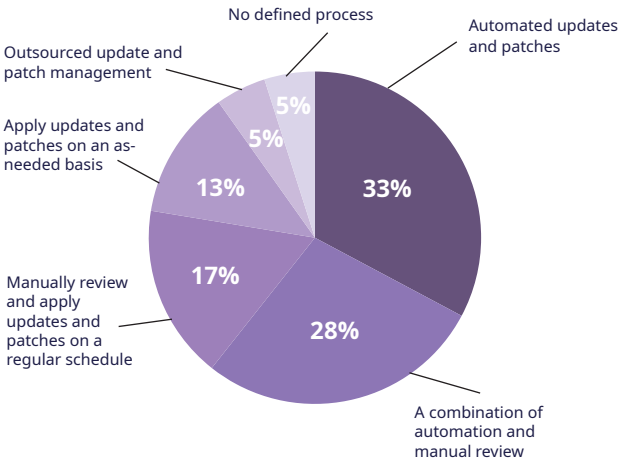
In contrast, with respect to security, the use of tools and analysis are common. Automated scanning tools are heavily relied on for detecting security vulnerabilities (76% of organizations). And while the majority do not take advantage of modeling, a significant share of organizations (40%) does use this analysis. Nearly one-third (30%) rely on manual processes and over a quarter (27%) rely on vendor notifications. Respondents could select more than one method their organization most relies on, so in many cases these manual approaches are supplements to the automation and modeling that predominate.

What methods does your organization use to control and monitor cloud/IT spending?



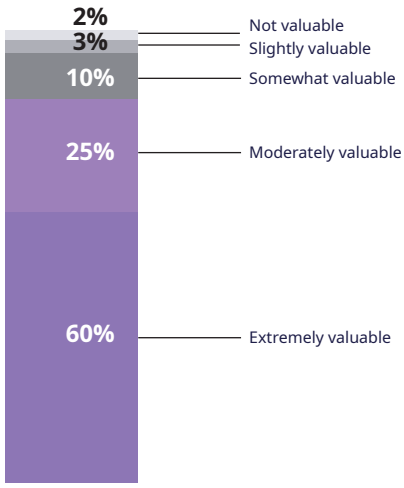
Organizations use an average of 2.4 methods to control and monitor cloud/IT spending, with centralized procurement processes being the most common (47%)—a method that, it is worth noting, does not explicitly employ cost-monitoring tools. The same can be said for methods such as pre-approved budget thresholds and regular audits, each of which over a quarter of organizations utilize. In the end, however, there is no clearly dominant approach, as other methods that do take advantage of tools such as cloud cost optimization platforms (35%) and automated cost monitoring tools (34%), are also utilized. Remarkably, about a sixth of organizations (16%) use no formal controls at all.

How do you typically handle system updates and security patches?



Well over half of organizations (61%) typically use automated system updates and security patches, either solely (33%) or in combination with manual review (28%). That leaves a significant share of organizations, however, not using any kind of automation—not the full 39% left over, perhaps, since 5% report outsourcing this function and it is likely that an outsourced security vendor will use automation. But we are still looking at roughly a third of organizations with no automated update and patch management system in regular use.

How valuable would it be for your monitoring and management solution to incorporate predictive analytics to help you identify and address system issues that are critical?



The vast majority (85%) of the infrastructure and security managers polled value incorporating predictive analytics into their monitoring and management solutions; the majority (60%) think it would be extremely valuable. This indicates a need for system management to be more proactive. But this may also reflect a desire for more efficient operations, given that remediation strategies tend to be less burdensome when risk factors are identified earlier.

Red Hat Insights continuously analyzes platforms and applications to help enterprises better manage their hybrid cloud environments and cut prolonged downtimes. Included in Red Hat subscriptions, Insights observes the health and performance of the IT estate using predictive analytics and deep domain expertise to reduce complex manual analysis and troubleshooting time from hours to minutes, including identifying security and performance risks, reporting on subscriptions, and managing costs.

By focusing on areas of operations, security, and business, Insights proactively alerts and directs administrators and stakeholders with actionable recommendations before an outage, security event, or overspending occurs. Teams stay ahead of critical operational issues, to free up resources and focus on delivering new features and innovation. Learn more about Red Hat Insights here.

This Techstrong PulseMeter is sponsored by Red Hat.
To learn more about Red Hat, visit redhat.com.