The Ultimate Guide to Hybrid Cloud Monitoring for Government

Table of Contents

It's a brave, new (cloud) world

The benefits of a hybrid cloud for government are compelling: scalability, agility, and cost containment, to name a few. It's why Gartner predicts that worldwide end-user spending on public cloud services is forecast to grow to $397.5 billion in 2022, up from $270 billion in 2020. Infrastructure-as-a-service (IaaS) and desktop-as-a-service (DaaS) should see the greatest growth as organizations face continued pressures to scale infrastructure that supports the demands of a hybrid workforce and moving complex workloads to the cloud.

When your agency combines the security of a private cloud with the expansive power and versatility of a public cloud, you get complete control over your data while leveraging the ability to quickly and cost-effectively scale your operational capacity.

But this also complicates today's already complex and dynamic application landscape. That's because application components each have their own stacks of layered dependencies across hybrid environments.

If your monitoring tools aren't optimized to monitor these components, maintaining visibility into your extended cloud environments can be fragmented and stressful. After all, you can't monitor and manage what you can't see.

In this guide, we'll explore proven strategies and little-known best practices that can help government agencies, regardless of size or mission, deliver a successful hybrid cloud implementation. With insights from Cisco AppDynamics' resident cloud experts, you'll learn how to achieve end-to-end visibility across your entire application environment, from a browser session request to a backend database call.

Demystifying hybrid cloud in government

Before we dive into the best practices associated with hybrid cloud monitoring, it's important to understand the basics. So what is hybrid cloud computing, anyways? And why are governments increasingly adopting hybrid cloud and multi-cloud infrastructures?

A hybrid cloud is a computing environment that uses a combination of services that run within on-premises, private cloud, and third-party, public clouds such as Amazon Web Services (AWS), Azure, or Google Cloud Platform (GCP), with data connectivity between all these environments. Forrester Research principal analyst Dave Bartoletti succinctly defines hybrid cloud this way:

> "One or more public clouds connected to something in my data center. That thing could be a private cloud, that thing could just be a traditional data center infrastructure."
>
> *Dave Bartoletti - Principal, Forrester Research*

Hybrid cloud deployment models bring many benefits to public sector entities that want the best of both public and private cloud environments. The biggest advantage is that it allows workloads and data to move freely between private and public clouds as operational or technology demands and costs change. Or when unexpected times of stress, such as uncontrollable natural disasters and pandemics, force a sudden shift in operations. Hybrid cloud empowers the flexibility, control, and options for data deployment and use needed at such times, giving governments greater resilience and the capability to continue the critical services their community depends on.

There is no one cloud rule for government since it encompasses such a wide variety of use cases, environments, and users. That's why so many are running their mission-critical application workloads across both private and public clouds. According to a March 2021 report by Forrester Consulting titled "Cloud-Enabled HPC And AI: A Spotlight On Government," hybrid is not the default, it's the preference for government IT leaders because it empowers them to optimize performance, significantly reduce cost, and increase security. As 451 Research said, "the future of IT is multi-cloud and hybrid." But with this rise in popularity, cloud spending optimization and visibility becomes more of a challenge.

Challenges of managing hybrid cloud

Recent surveys show that one of the main concerns today in managing and monitoring workloads in the public cloud is achieving complete end-to-end visibility into software and hardware stacks deployed across on-premises infrastructures and private and public clouds. Research from Keysight Technologies reveals that 65 percent of IT professionals are concerned about their visibility into data and application traffic across on-premises and cloud systems.

While the benefits of using hybrid cloud in the public sector are clear, challenges remain. Issues that make it difficult to manage and monitor hybrid cloud environments include:

✓ Limited visibilty

Why is it so difficult to monitor performance issues and isolate the root cause of a problem without impacting operations? One reason is that when your applications are distributed, you end up with a huge amount of performance data, application data, infrastructure data, network data, and so on. This is especially true in government due to the siloing of networks that often occurs due to differing mandates and tools required by special work environments and/or uses. With data distribution based on these unique needs, it's difficult to trace what happened at each step. Managing the performance of the entire application can end up being a largely prolonged manual effort, with significant blind spots and gaps along the way.

When public sector applications are distributed, you end up with a huge amount of performance data, application data, infrastructure data, network data, and so on as well as issues due to differing mandates, use environments, and tools. This can create significant blind spots and gaps in your visibility and ability to manage everything efficiently.

✓ Multiple silos

Cloud providers offer dashboards and other tools to monitor their respective cloud-native services and infrastructure. Unfortunately, these tools don't provide the ability to combine performance data throughout the application stack and across multiple hybrid cloud environments. And as the type and scale of government services grow, as witnessed during the COVID-19 pandemic, the issue will certainly become more intense.

Without this capability, you can't get a comprehensive view of how your applications work and their direct impact on your operations. In the end, you are creating siloed monitoring strategies that impact your overall application performance and mean-time-to-resolution (MTTR) metrics. That's why so many cloud-native tools have common shortcomings when it comes to hybrid cloud and multi-cloud application monitoring in a public sector setting, including:

- Narrow scope: Typically IaaS-focused, these siloed monitoring solutions can cause huge gaps in visualizing application health.
- No code-level insights: Without diagnostic capabilities that enable you to identify root cause down to the individual line of code, MTTR suffers.
- Coding required: Application visibility is enabled via software development kits (SDKs) that often require manual coding changes.
- Lack of business context: Monitoring is focused on technology only and often does not provide any context to track business outcomes.
- Manual anomaly detection: Cloud monitoring tools are primarily designed to collect metrics, leaving it up to the user to come up with the definition of the norm and detect anomalies manually.
- Limited network visibility: These tools don't provide a view of network outages across ISPs, public cloud, UCaaS, and edge service providers (ESPs), critical information when dealing with a real-time breach or other security threat.

At the same time, there is no way cloud-native monitoring tools like Amazon CloudWatch, Azure Monitor, or Google Stackdriver can be ignored by government IT staff involved in the daily management of their cloud based operations. They provide observability, monitoring, and operational data in the form of logs, metrics, and events, providing access to cloud resources and services that run on the cloud. Interoperability with cloud-native monitoring services is critical for end-to-end hybrid cloud visibility.

✓ Vendor lock-in

The public sector has historically relied upon a mix of solutions for IT, and that hasn't changed with their move to the cloud. Legacy IT, "free apps" and other random issues all find their way into the mix. This makes things more difficult due to the lack of cloud monitoring integration. And you may often find that any monitoring tools only work with the respective vendor's technology.

As a result, you lose control over the data and infrastructure that power your mission-critical applications. Not having complete control over aspects like security, uptime, and overall infrastructure management can be worrisome. When you're depending on a single vendor, your servers, data, networking, user management, and more are in the hands of one company. If something goes wrong it can be detrimental to your community, impacting your ability to provide critical services or respond to emergencies.

There's also the risk that the one cloud provider-specific tool may not meet your multi-cloud or hybrid cloud monitoring goals in the future. The difficulties and costs associated with switching to a new cloud vendor are significant and understandably of concern to your agency's IT manager when deciding to move to the cloud. For this reason, there's a growing need for a more portable application architecture and monitoring strategy for the public sector that frees them from a specific style of application development.

The unwritten rules of hybrid cloud monitoring

The immediate solution to these challenges is simple: Obtain complete, end-to-end visibility into every action across the multiple types of cloud environments government agencies might utilize.

Simple in theory, that is.

In practice, this means taking into consideration everything that may affect your operations due to application performance issues caused by either the application itself —or any layer of the underlying infrastructure, including middleware and databases, as well as external events out of your control. This alone is challenging, but coupled with today's evolving user and operational needs, the task is seemingly impossible.

So, what does efficient hybrid cloud monitoring look like?

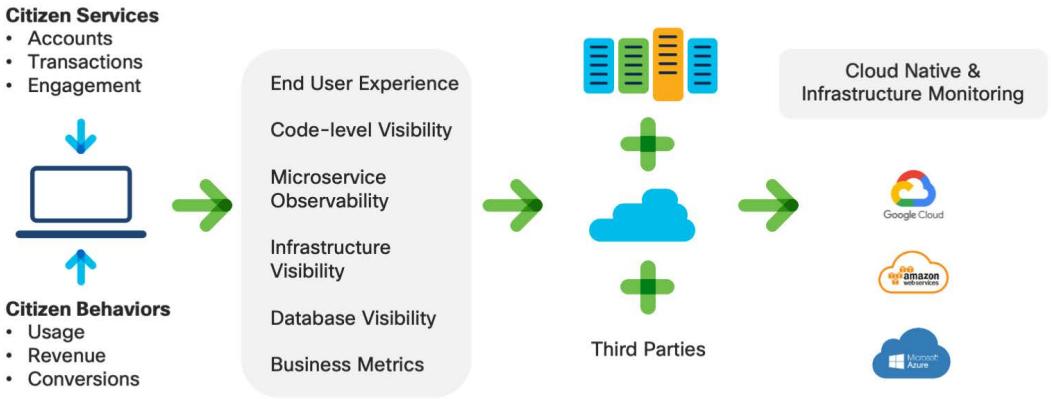
Here are five little-known but game-changing best practices that government IT teams can use for monitoring their hybrid cloud infrastructure:

Rule #1: Think application first

In hybrid and multi-cloud environments for government, any domain of infrastructure or application services may become the spot where an issue originates. But it's possible that the issue may be impacting your users and mission critical operations. This is why every action across these environments must be correlated and monitored end-to-end.

An application-centric approach to monitoring is an excellent strategy for achieving comprehensive, intelligent visibility into critical actions. With Cisco AppDynamics, government IT staff can expand the platform's level of visibility and represent applications through a single lens as they exist across both public and private clouds.

You can also map individual applications to their desired mission or citizen outcomes by leveraging Cisco AppDynamics Business iQ. It delivers business performance monitoring and observability for every layer of your tech stack, that you can work as one to prioritize what matters most. This includes the capability to create mission metrics and map them to application metrics.



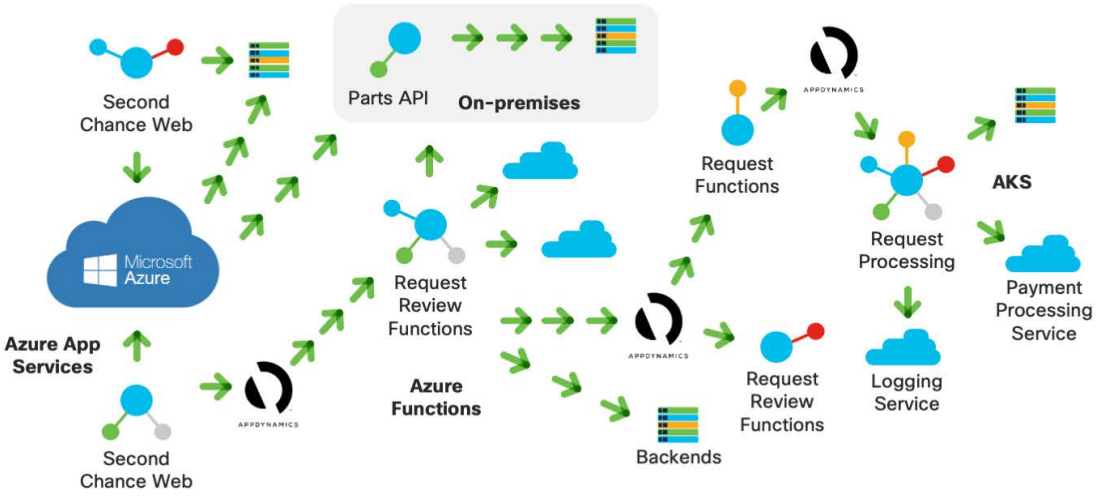
Rule #2: Keep it simple and secure

Simple yet diverse

Today you may be running your application within a combination of servers in your data center and in the public cloud, which may expand and contract as demand within your operations and community of users changes. This may also be impacted by large scale, unexpected events that result in longer term changes. So you need the ability to move and redesign your workloads to where it makes the most sense from a technical and operational perspective. This is where hybrid cloud adds strong value to government IT since it allows agencies to incrementally modernize their applications. At the same time, it also poses a unique challenge.

Often presented with a blend of legacy and next-generation technology environments, it is important that government IT teams reduce complexity with unified monitoring. This means choosing an application performance management (APM) solution that can provide deep visibility into legacy and modern application architectures and their supporting infrastructure systems. Cisco AppDynamics currently supports over 200 integrations—including technologies and platforms across on-premises and public cloud—and can be leveraged to:

- Monitor microservice workloads across multiple platforms
- Monitor serverless applications like AWS Lambda and Azure Functions
- Integrate seamlessly with cloud vendors' performance data
- Establish easy-to-understand visualizations
- Establish end-to-end transaction tracing correlated with the user journey
- Support legacy technologies and applications (C++, Tibco, SAP)
- Gain visibility into multiple platforms (VMWare, Azure, AWS, Linux).



Example: How a hybrid app can be monitored with Cisco AppDynamics across on-premises and Azure public clouds.

Secure with RBAC

For public sector organizations, Role-Based Access Control (RBAC) is a critical capability that monitors applications in a hybrid cloud. With RBAC, your agency can gain complete visibility and oversight into permissions. It provides the ability to easily manage who has access to your cloud-based resources, what matrices or application stacks can be accessed by users, and what types of actions users can perform with the resources they are permitted to use. As bad actors, including insider threats, increase attempts to access government networks like yours, implementing RBAC helps make a breach more difficult to implement and can also limit the scope of any breach. And for day-to-day operations it can help increase the efficiency and security of your operations by reducing unnecessary or accidental access and network activities.

Federally recognized FedRAMP Authorized level of security

Cisco AppDynamics delivers FedRAMP Authorized performance monitoring for mission-critical applications, critical for governments that must provide critical services to citizens every day. Cisco AppDynamics is purpose-built for government agencies to efficiently manage applications and drive cloud adoption, while maintaining high security standards.

Rule #3: Empower application teams

Enable end-to-end visibility to deliver a seamless hybrid app experience

Today's governments must deliver a flawless citizen experience to promote transparency, increase engagement and build trust with residents. When digital citizen services don't deliver a first-rate experience—one that is seamless and issue-free—the impact can be profound. It can alter public perception of how well government is working, reduce the quality of life for residents and, unfortunately, impact public health and safety in your community.

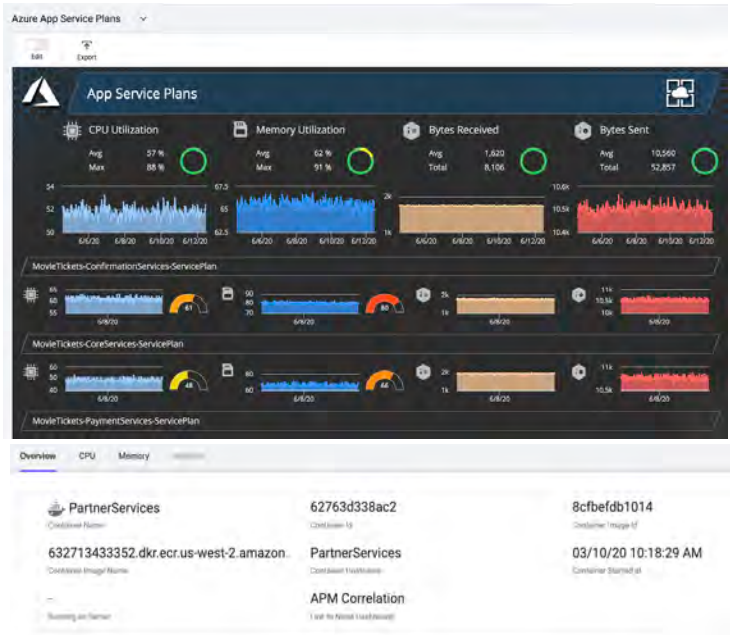
To meet citizen expectations, your agency's application team must be able to correlate the user experience (both staff and constituent) with application and infrastructure in hybrid deployment. Experience Journey Map (ExJM) from Cisco AppDynamics solves this problem, giving application owners, IT operations, and developers alike end-to-end visibility into the user journey.

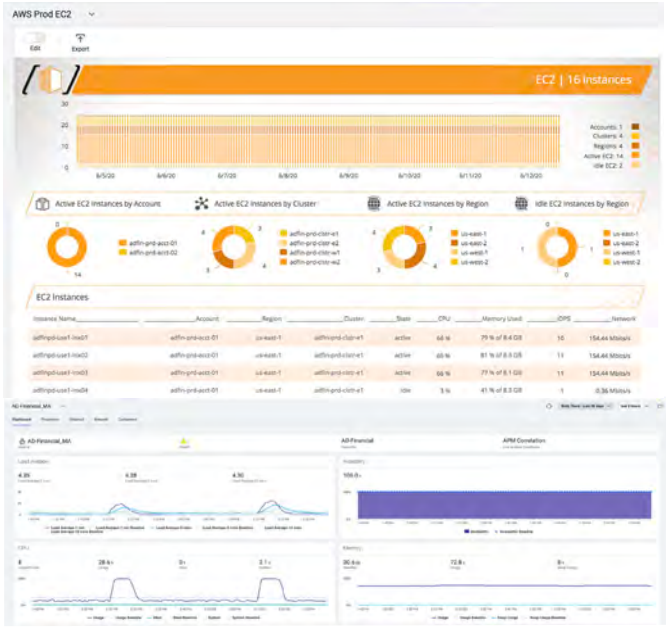
Providing application teams a performance-lens view of user behavior, ExJM allows you to identify problem areas and determine root cause more quickly. It provides deep insights into how users interact with applications across browsers or mobile devices, allowing teams to identify hot spots in the user journey as soon as they appear. User experience glitches can be automatically mapped to application flows, enabling detection of performance anomalies across all your cloud services. With the power of machine learning, you can also diagnose the root cause of an emerging issue before it impacts a broad segment of your users and operations.

Gain side-by-side visibility of hybrid infrastructure

In the public sector, getting the right insights from your hybrid environment can fuel intelligent decision-making that drives rapid issue resolution and help predict future performance. Cisco AppDynamics provides integration into a number of commonly used public clouds and virtualization platforms used on-premises, and can also be run on bare-metal, on-premises servers.

This means you can remove the dependencies of using cloud-native monitoring services to monitor your modern application services running in the cloud, while still monitoring your on-prem secure legacy applications individually. This approach also helps break down the silos so common between government agencies and departments, allowing you to identify, fix, and resolve issues faster.

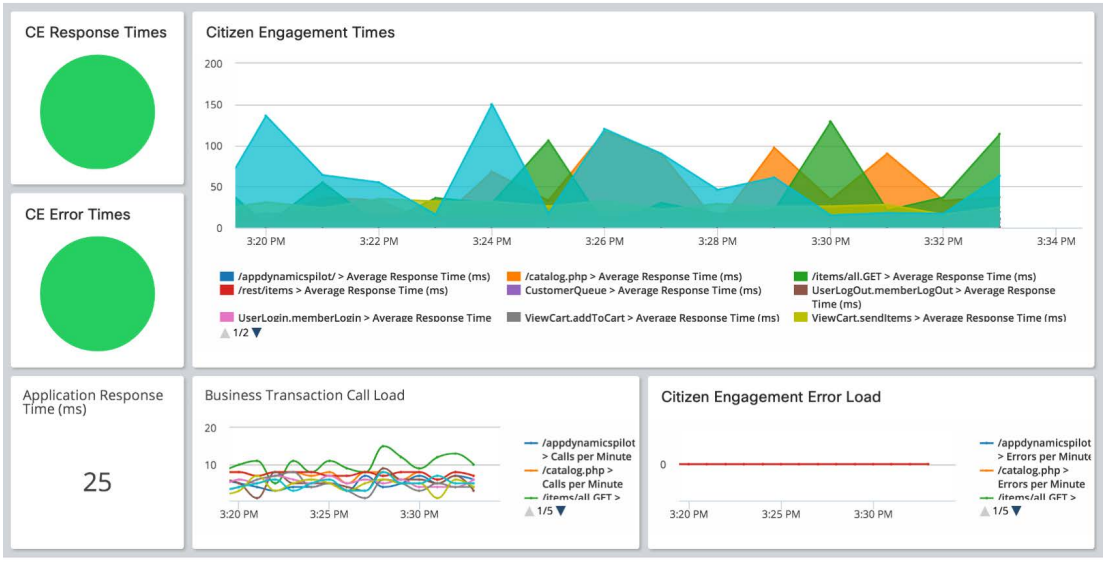


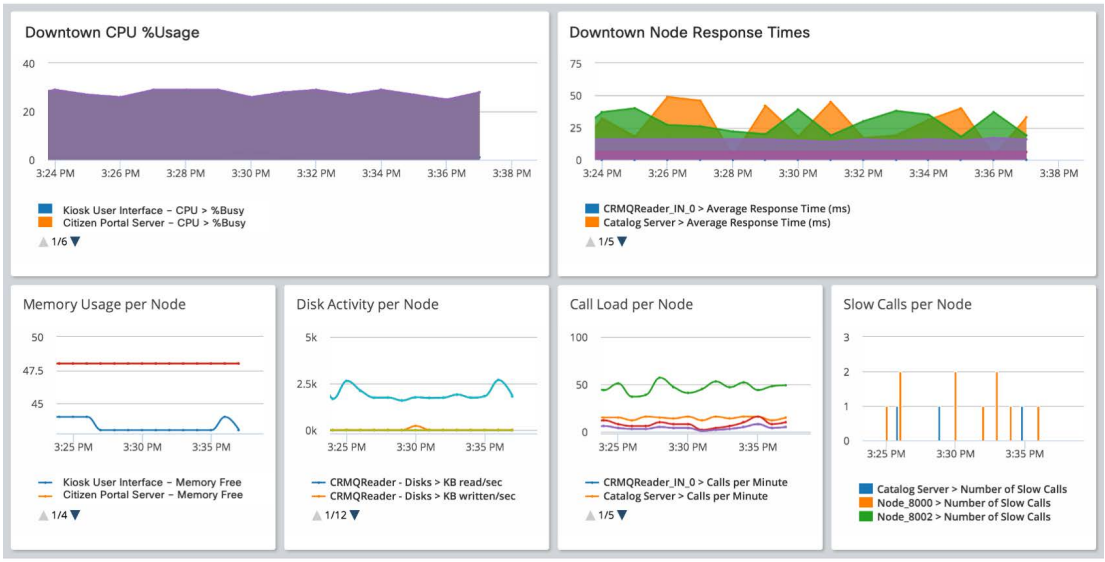


Rule #4: Practice continuous performance testing and baselining

The ability to deliver a lean hybrid cloud in days or weeks is an ambitious goal for any government-run IT team. Getting buy-in from all stakeholders, ensuring integration across various platforms/user groups, and doing so all within budget is a big challenge. That's why selecting which workloads to run on your private or public cloud requires trustworthy metrics.

Metrics are a crucial component of any government hybrid cloud strategy. One of Cisco AppDynamics' core strengths is its ability to compare workloads and platforms for effectiveness. When a new application works effectively in your hybrid cloud infrastructure, your agency's users and leaders (including political leadership) gain confidence in your investment and quickly bring additional workloads into the new model. By using Cisco AppDynamics to trace an action, such as those related to citizen inquiries or billing transactions, your agency's IT team can easily justify where and why a workload is running in a particular segment of the hybrid cloud environment.





Rule #5: Get the right tool for the job

As with any of your IT investments, when choosing a hybrid cloud monitoring solution for government use, it's important to choose the right tool for the job. Just like you wouldn't use a screwdriver to hammer in a nail, it's important to assess each tool in your hybrid cloud toolbox for its purpose, strengths, and weaknesses.

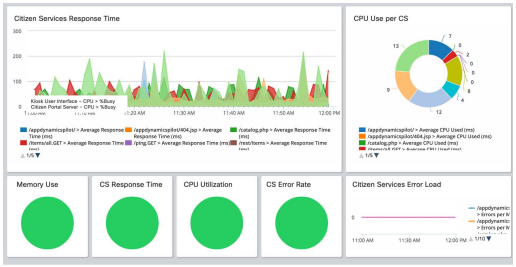
Full stack observability

Today's government IT environments extend beyond four walls and across campuses, so they're deeply interconnected with Software-as-a-Service (SaaS) applications, cloud-based services, and many service providers across the global Internet. Every day, users access externally hosted applications over hundreds of networks outside of your control. You may not own these networks, but you still own service delivery outcomes—outcomes that can be impossible to influence when you have no visibility outside your network. When users inevitably experience poor performance or service disruptions, it can take hours or even days to determine if the problem is your network, someone else's network, or the application.

Our unique approach to full stack observability (FSO) starts at the application layer where Cisco AppDynamics provides our public sector customers the broadest and deepest visibility into their IT stack and correlates everything that impacts the application experience. Our strategy extends beyond just domain monitoring, with cross-architecture integrations between Cisco AppDynamics, ThousandEyes, Intersight, and Secure Application. Together, these create a FSO platform to transform your operations.

Cisco® ThousandEyes Internet and Cloud Intelligence delivers end-to-end visibility from your campus networks to Internet, SaaS, and cloud-based services that are critical to government operations but outside your direct control, enabling you to meet service commitments and ensure excellent user experience. Combined with the Cisco Catalyst 9000 Switches, ThousandEyes helps you find and solve problems faster for flawless network and application experience. Cisco AppDynamics also integrates with Cisco Intersight to provide a portfolio of services that enable intelligent visualization, optimization, and orchestration for applications and infrastructure across your hybrid environment to bring your teams, tools, infrastructure, and apps together.

Actionable alerts



With an effective integration between your performance intelligence platform and ITSM system, actionable alerts can easily be viewed and acted on. To help public sector IT teams get their apps back up and running as quickly as possible when incidents occur, Cisco AppDynamics integrates with Moogsoft, ServiceNow ITSM, Cherwell, BMC Remedy, and configuration management systems such as Evolven to manage incidents, problems, and changes. By combining Cisco AppDynamics' granular visibility of applications with incident management capabilities, your IT team can triage user-impacting events before they affect users.

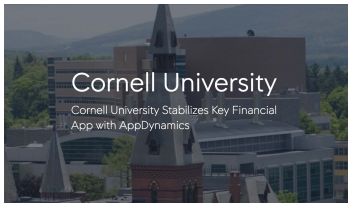
Configuration management

Automating the management of monitoring configuration across hybrid workloads is key to speed and agility. Your monitoring tool configuration should follow the same mantra of configuration as with code. Integrate your pipeline orchestration tools to signal to your APM software when something is happening. Signal the start and completion of jobs that deploy software and execute tests. Doing this will ensure you can overlay events that change the environment with performance data, enabling you to see the impact of the change in real time.

Why Cisco AppDynamics?

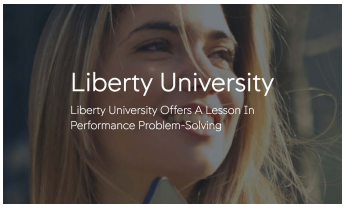
Public Sector customer stories

Cisco AppDynamics is the #1 fastest-growing application performance monitoring solution in the world. What makes us unique is our easy integration into Cisco architecture and our unrivaled path to drive the AIOps solution for hybrid IT architecture. Cisco AppDynamics is empowering the public sector with AI-powered insights and automation to drive the future of performance monitoring in government IT.



Cornell University is stabilizing key financial applications to improve transactions, using Cisco AppDynamics.

Cisco AppDynamics is helping power the California Natural Resources Agency to enhanced IT performance.



Liberty University is enabling visibility across their entire network and application environment with Cisco AppDynamics.

Navigating the multi-cloud haze

Reliance on multi-cloud and hybrid cloud environments by federal, state and local governments is on the rise, bringing new challenges for IT professionals. To retain visibility and control in your hybrid cloud environment, you need a new approach to monitoring.

With Cisco AppDynamics, you can empower such an approach and gain end-to-end visibility across your hybrid cloud infrastructure to reduce complexity, deliver a seamless user experience for all users (including staff and citizens), and directly correlate technical issues to operational performance. Whether your applications are running on-premises, in the cloud, or both, Cisco AppDynamics provides deeper visibility to find bottlenecks, address inefficiencies, and accelerate performance. Together, these can work to improve the reliability, security and response times of mission-critical services that governments typically provide residents in their communities.

About Cisco AppDynamics

Cisco AppDynamics is the Application Intelligence solution that empowers public sector organizations with real-time insights into application performance, user performance and operational performance. This lets them move faster in an increasingly sophisticated, software-driven world.

Cisco AppDynamics' integrated suite of applications is built on its innovative, enterprise-grade App iQ Platform that allows governments to make faster decisions that enhance citizen engagement and improve operational and business performance. We're uniquely positioned to enable the public sector accelerate its digital transformation by actively monitoring, analyzing and optimizing complex application environments at scale.

To learn more about Cisco AppDynamics and to start your free trial, visit: cisco.com/go/appd.

Discover how Cisco can help strengthen community and resilience for all at cisco.com/go/stateandlocal.