White Paper

Citrix App Delivery and Security Service

A paradigm shift for IT modernization

Table of Contents

Secure application delivery at a crossroads

It is time for IT organizations to fundamentally re-examine how applications are delivered and secured. Two key trends have now placed business application delivery at a crossroads that can threaten or accelerate the growth of the underlying business:

Application experience is the new currency: Application experience is the new currency for business because it profoundly impacts employee experience, customer-perceived differentiation, and the ability to build intimacy and engagement with both employees and customers.

Hyper-transition to cloud and SaaS: The global pandemic created a new urgency for organizations to transition applications to cloud and SaaS for the elastic demand, global reach, and uniform access they provide. The big question is how fast can organizations make the transition.

Business pressure to deliver the best application experience and to accelerate application migration to cloud are creating pressing challenges for IT organizations.

- **IT is in perpetual catchup mode with business:** IT complexity continues to increase with cloud and SaaS in spite of DevOps and continuous delivery adoption.
- **The state of the internet remains a blind spot:** Applications depend on the public internet because both they and their users are globally distributed. Additionally, the internet is effectively the corporate WAN. Yet application delivery infrastructure cannot see fast-changing internet conditions and therefore cannot react to them.
- **Fragmented application and security solutions:** Application security is more important than ever due to globally dispersed users and applications. But the complexity of protecting such fragmented, dynamic environments is resulting in more vulnerabilities that are easily exploited by advanced attackers.

20 years of innovation

2001 First single-pass load balancer for better performance: A huge step in software design that allowed general-purpose CPUs to meet the performance needs of the expanding internet without specialized hardware.

2009 First multi-core ADC for scale: NetScaler broke the barrier of single-core performance, enabling customers to scale their ADC performance without adding footprint and installation time for new boxes.

2010 First fully featured, virtual ADC for cloud: NetScaler VPX brought TCO reduction to the masses. With no hardware, NetScaler VPX provided rapid scaling, availability, security, and performance optimizations. Application behavior could be tailored as applications were provisioned — wherever and whenever they were needed.

2015 First full-featured ADC in container: Provided operational consistency between monolithic and microservices-based applications. This enabled customers to accelerate their application modernization.

2016 First pooled-capacity licensing for flexibility: Enabled customers to instantly and confidently shift ADC capacity where needed for easier application migration to public cloud, providing operational consistency.

2017 First cloud-based ADC management: Citrix Application Delivery Management (ADM) provided a unified console from which administrators could monitor, troubleshoot, and orchestrate ADCs in hybrid and multi-cloud environments.

2019 First bare metal ADC for performance: Citrix launched Citrix ADC BLX, the world's first bare-metal ADC with full DPDK support for superior performance.

Citrix: A pioneer in application delivery solutions

For more than 20 years, Citrix has led numerous innovations in application delivery and security solutions and is well-positioned to offer a transformational solution.

Now Citrix is launching a game-changing solution for at least the next decade: Citrix App Delivery and Security Service.

Introducing Citrix App Delivery and Security Service

Built on human principles

Citrix App Delivery and Security Service is a quantum leap that radically simplifies application delivery and security using an intent-based, self-healing, and internet-aware solution. It is built on four human principles that have shaped human progress through the modern era: "Intent based," "always learning," "always adapting," and "always protecting."

- **Intent based:** The vast majority of human action is driven by high-level intent, such as planning to take a vacation. The many steps taken to embark on a vacation—choosing locations, dates, mode of travel, lodging, itinerary, and budget—can result in a huge number of actions that begin with simple intent. Citrix App Delivery and Security Service is very similar. It automatically translates intent, stated as declarative outcomes, into dozens of policies and hundreds of configurations for ADCs.

  Intent-based policies and configurations remove the guesswork from orchestration, ensuring agility, radical simplicity, and optimal user experience. Simply define your desired outcome, and Citrix App Delivery and Security Service will configure accordingly. For example, you may define a maximum acceptable application latency threshold for users in a certain geography. Taking into account the many factors that contribute to latency between users and the app server locations, the service automatically redirects users to the best application servers.

  However, despite the best-laid plans, conditions can change—whether that's a flight cancellation that delays your vacation or an internet bottleneck that slows your application traffic. That's why it is essential to have continuous enforcement of declarative intent in response to changing conditions. This is where the next three human principles come in to play with application delivery and security.

- **Always learning:** A traveler may learn about changes that affect his vacation from many sources such as the hotel, airline, concierge, and his own real-time observations. Citrix App Delivery and Security Service continually learns about the complete app-to-user environment, including server conditions, ADC status, internet state, and emerging cyberthreats. It uses 360-degree visibility to monitor anomalies and establish such baselines as "normal latency" between geographic regions.

- **Always adapting:** Humans can achieve incredible proficiency by combining learning with adaptation in a continuous loop. This is easy to see in sports, where beginners can become pros by repeatedly adjusting their approach as they monitor results in varying situations. Citrix App Delivery and Security Service also adapts its response to the latest conditions, continuously and automatically. In large deployments, many things can go wrong between global users and distributed applications.

  The service's sophisticated analytics differentiate trends from anomalies and automatically decide whether to update policy thresholds, send alarms to IT, make recommendations, or all three. Citrix App Delivery and Security Service self-heals by adjusting resources, traffic paths, and more on a global scale so that your application delivery infrastructure will adjust to meet your defined intent.

- **Always protecting:** Humans protect what is most precious, such as friends, family, and finances. For businesses, their applications and APIs over which data is shared are their most valuable assets and must be protected from cyberattacks and threats. Citrix App Delivery and Security Service expresses security policies as intent, for a variety of threat vectors, including bot, API, and DDoS attacks. It provides single dashboard for threat visibility, security policies and automatic enforcement actions, so that IT teams can transition their apps to global access and multi-cloud with confidence.

The combination of these four human principles creates a paradigm shift in delivering applications and security. The intent-driven approach dramatically shrinks "Day 0" thru "Day 1" activities, which include plan, design, install, configure and deploy, because Citrix App Delivery and Security Service does most of the background work automatically. Subsequently, continuous learning, adapting, and protecting drastically simplify "Day 2" operations and orchestration because Citrix App Delivery and Security Service transforms change management from a manual, repetitive, and error-prone process to one that is automated, scalable, and error free.

With Citrix App Delivery and Security Service, IT can finally be in lockstep with the business instead of in perpetual catch-up mode. Now IT can focus on business outcomes and innovation rather than the day-to-day syntax of application delivery. At Citrix we believe that machines should manage the app delivery and people should define the business intent.

Let's look at how Citrix App Delivery and Security radically simplifies application delivery to speed up the software development lifecycle.

Intent based and awesomely automated

The process of migrating apps to hybrid cloud and multi-cloud is filled with lots of manual configuration and, more significantly, guesswork. Here are the typical steps for a first-time cloud deployment:

Day 0: Plan and design

1. Select the right EC2 instance type for your ADC. There are 200+ different types of EC2 instances, so choosing the right one for your workload is not easy.
2. Select the right ADC instance type and license it. Guessing the right size you will need in terms of throughput or processing power can be challenging.

Day 1: Configure and deploy

3. Manually configure the ADC to add all the back-end application servers. Determine how you want your traffic distributed and what health monitoring you want.
4. Manually publish your application to a DNS (like Route 53) so it's reachable.
5. Guess the thresholds to set for CPU, memory, and network throughput for auto-scaling so that your systems flex to meet your expected demand. Guessing often results in mis-timed actions, such as auto-scaling too early or too late.
6. Repeat steps 1-5 many times as the business needs change.

With Citrix App Delivery and Security Service, almost everything is automated. We refer to this degree of automation as "awesomely automated" because it removes nearly all manual effort and complexity from every step starting with planning through deployment. In the above example of a first-time cloud deployment, Citrix App Delivery and Security Service interprets a simple intent statement to set up the cloud app delivery and calculates the requirements so you don't have to:

1. Citrix will automatically use the right ADC instance and use available licenses.
2. Citrix will translate your intent into policies and automatically create a config to deliver your application.
3. Citrix will automatically publish your application domain to a DNS like Route 53.
4. Citrix will auto-scale when it's necessary to meet your application demand. The concept of defining thresholds no longer applies.
5. And when your requirements change, the service will simply adjust according to your new intent.

Awesome automation can increase operational efficiencies by up to 60 percent for IT teams. Most importantly, there is no guesswork and no error-prone manual configurations that complicate your application deployment and delivery.

Always learning and adapting

Beyond the application delivery's initial state, intent needs to be enforced continuously as conditions change. End-to-end continuous app delivery is complex. Outages or degradation can occur anywhere between thousands of users and applications, especially when user demand surges. And systems can remain overprovisioned after demand drops.

Continuous optimization

Today a large portion of Day 2 operations is spent optimizing application delivery because it is manual, repetitive, and error prone. IT teams rely on years of individual experience and tribal knowledge. It is nearly impossible to offer end-to-end service-level agreements because resource and network conditions will surely change or deteriorate and will take time to manually detect, analyze, and fix. As insurance, organizations will often opt to keep extra resources available, quickly driving up OpEx.

With Citrix App Delivery and Security Service, operations and orchestration are drastically simplified. The service continuously and automatically optimizes app delivery, end to end, so that it remains aligned to the business intent.

Self-healing

Citrix App Delivery and Security Service self-heals the user experience by automatically adjusting many parameters. For example, here are three areas where application experience is prone to degradation:

1. **App server degradation:** When an app server is no longer functioning optimally, the application experience is commonly perceived as sustained slow response. The service continuously monitors the server health and performance to identify performance issues. Although other services or devices can do this, Citrix App Delivery and Security Service can also automatically remove poorly performing servers from the app server pool to prevent requests from being sent there.

2. **ADC exhaustion:** When user demand for an application increases rapidly, ADC exhaustion can occur. New service rollouts and marketing and sales events like Black Friday and Cyber Monday can cause demand to spike. Significant weather events and natural disasters can cause a shopping rush for provisions.

    - Citrix App Delivery and Security Service can automate the addition of ADC resources to cope with increased demand. The service will automatically orchestrate the addition of a new ADC and configure it according to intent and policies. This is true auto-scaling the way it was meant to be.
    - When demand drops, the service automatically removes unneeded resources, saving you money.

3. **Internet state changes:** Internet traffic typically hops over a few networks including edge networks managed by ISPs and CDNs. Brief outages in these networks are common and occur primarily due to configuration errors, human errors, and demand surges. Regardless of the cause, they are perceived as worsening latency, availability,

and throughput.

- Citrix App Delivery and Security Service continuously monitors the state of the internet and automatically redirects requests to the best site or PoP for each individual user to ensure the best possible user experience.
- The service provides comprehensive visibility and real-time self-healing actions to maintain an optimal user experience.

Citrix App Delivery and Security Service monitors and acts on end-to-end traffic path, as needed, automatically. This broad adaptability can provide a more exceptional application experience for all users than was ever possible before. And it can do so while drastically reducing the need for IT intervention.

Moreover, the service offers IT teams a choice in the level of automation to use, depending on their orchestration complexity, policy evolution and comfort level.

The level of automation you choose is similar in concept to assisted driving where you can use the navigation system to help you drive the car to your destination or let the car drive for you.

Automation level	Decreasing manual effort
1. Alert	Admins troubleshoot manually
2. Alert and recommend	Admins review and plan detailed actions
3. Alert, recommend, one-click fix	Admins review and click for immediate result
4. Fully automated	Zero intervention

Today IT spends most of its time monitoring global networks and troubleshooting and fixing problems. But manual operations are simply not sustainable as more applications are migrated to the cloud. Citrix App Delivery and Security Service continuously optimizes your application delivery infrastructure from end to end, ensuring the efficient use of resources and an optimal application experience for your users.

Now, let's examine the power of combining internet-state visibility with self-healing application delivery.

Self-healing the user-experience

Globally distributed enterprise applications can easily degrade when it comes to performance, security, scale, and availability. Diagnostic alarms are often too numerous and ambiguous to be helpful. IT Ops must notice the problem, remove the servers from the traffic, permit scaling of the load balancers, and reassign the traffic to alternative servers.

Citrix App Delivery and Security Service is self-healing and continually monitors, diagnoses, and remedies application degradation.

Citrix App Delivery and Security Service will:

- Automatically remove a degraded server from the load balancing pool or auto-adjust the load balancing algorithm to improve performance.
- Automatically add and configure additional ADS instances when service demand exhausts ADC systems resources.
- Auto-redirect traffic globally to a new app server added by the cloud provider or IT Ops.

Internet-state visibility: A revolution in the app experience

The state of the internet is a major blind spot for application delivery. By design, the internet finds alternate paths around outages in individual networks. But in the interim, it is common for users to experience degradation in latency,

availability, and throughput. Additionally, IT teams have no control over the internet or its state. Traditional global server load balancing attempts to mitigate issues that degrade app delivery across the internet, but it is itself blind to the changes that occur across the internet.

Citrix App Delivery and Security Service has granular real-time visibility of the state of the internet so that self-healing actions are correct and immediate. It can even anticipate trends to recommend broader actions proactively. To achieve this visibility, the service incorporates Citrix ITM technology, which monitors up to 10 billion data points a day from 1 billon users across 50,000 networks throughout the world. The data is continuously crowd-sourced from nearly all edge networks, including third-party CDNs and PoPs. It creates a real-time, up-to-date map of the user experience.

The service automatically analyzes this data, establishing new baselines, updating anomalies, and projecting trends. Remediation can be automatic, or the service can provide IT with recommendations to improve planning and design. As we will see in the following two examples, the improved engagement of users interacting with your business applications can be cumulative and profound over time.

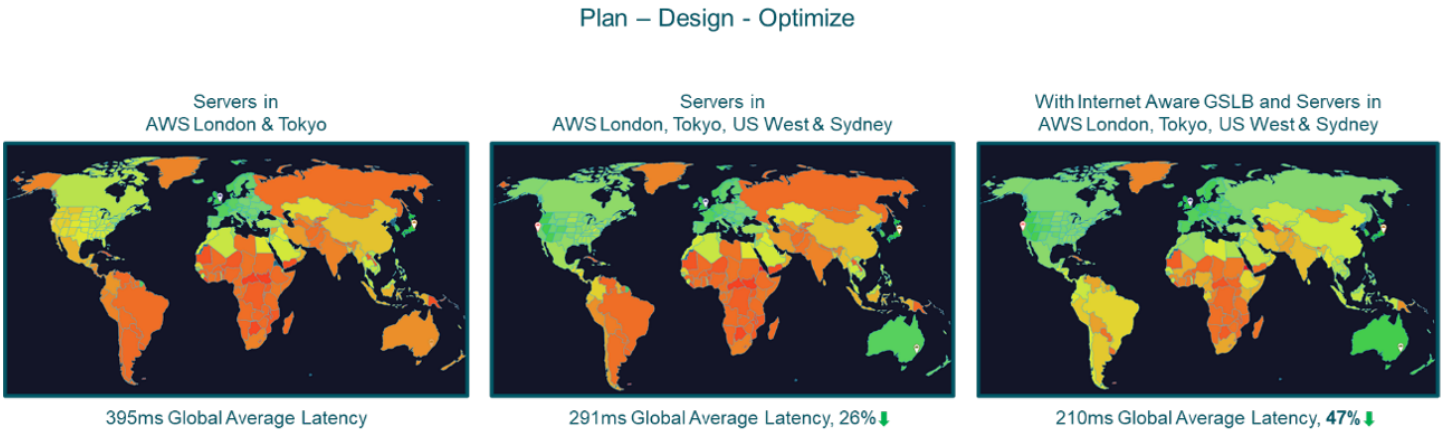
Planning for your app hosting locations

A big question when planning an application deployment is where to host the application servers. Today the location decision is an educated guess and yet it is one of the most consequential. Between US West, US East, London, Tokyo, and others, there is no way to know for sure which will provide the best application experience to a specific user base.

No existing tools can measure the differences for a deployment that has not yet occurred. Nor can they assess the net improvement among locations with different strengths in latency, availability, and throughput. Nor can they help with the choice between a single central location or multiple smaller ones. Finally, they cannot account for emerging trends due to changing conditions or a shifting user base.

Citrix App Delivery and Security Service removes nearly all of these uncertainties. Before deploying an application, you can plan out different scenarios based on real-time internet state and emerging trends. For example, the service can provide accurate visibility for the following scenarios:

- **Scenario 1** What if I open two AWS PoPs in London and Tokyo? What is the average latency for user across the globe or in specific countries? The service provides a latency heat map across the globe, which shows the relative experience of each country's users.
- **Scenario 2** What happens if I add two more PoPs in US West and Sydney? How will it impact the overall app delivery in specific countries or globally?
- **Scenario 3** What happens if I change the traffic redistribution mechanism? How does switching between round



robin, proximity, and Citrix-optimized delivery change the user experience?

Best of all, the results for each of these scenarios will be generated in seconds so that IT can realistically model many different "what if" scenarios. And the visibility is not restricted to a single cloud or CDN. Public cloud providers like AWS, Microsoft, and Google can only provide visibility for their respective partner or managed networks. Citrix App Delivery and Security Service has visibility into them all.

Planning for additional PoPs or server sites is a major Day-0 activity with long-term consequences. The service makes Day-0 site planning a natural extension of Day- 2 continuous optimization, because the service sees trends over time, that drive its recommendations as it tries to maintain the initi

The first internet-state aware GSLB

Global server load balancer (GSLB) innovation is falling behind the needs of globalized application delivery. Its core function is to spread traffic load evenly across geographical regions where app servers are located. To do that, it uses basic rules like geographical proximity, where users are assumed to be near servers if their respective IP ranges are geographically close.

But current GSLBs know nothing about the actual internet conditions between the user and the servers. Temporary internet congestion occurs frequently, even between users and applications in the same geography. This can happen due to outages in other geographical locations (causing that traffic to find alternate paths), configuration errors in CDNs, and demand spikes. Transient internet congestion increasingly affects users and apps as they become more globally distributed. GSLBs increasingly fail to deliver the expected response and sometimes make things worse.

Citrix App Delivery and Security Service is the world's first GSLB with actionable internet-state visibility. Now it is possible to optimize for the state of the internet and the state of the server depending on the degree that each affects response. For example, if a user is located in Japan and the nearest available PoP is in Seoul, the user may in fact be directed to Seattle if it is in fact the "closest" PoP in terms of real latency.

The service knows the best PoP for each individual user based on the lowest latency from every PoP to the user's ISP network. Within the best PoP, the service will steer traffic to the best application resource—usually the server with the fewest connections—to minimize the response time. Moreover, the service can monitor where

Making global applications adaptable to the changing Internet

In 2021, the lack of website responsiveness and availability and slow throughput are still affecting major online brands and their bottom lines. All enterprise applications that are accessed globally by employees and partners also experience similar issues.

The internet is a big contributor to less-than-optimal application performance because regional network congestion is frequent. Additionally, an outage in one region can create congestion in others.

Citrix App Delivery and Security Service optimizes the user experience based on real-time conditions as well as emerging internet conditions that are informed by historical trends. The service use intelligent traffic management (ITM) to:

- Identify root causes of deteriorating user experience—such as an ISP network failure or a cloud outage—and steer user requests to sites with the fastest overall response.
- Analyze latency and throughput trends that may impact future experience and recommends the best new regions for applications, CDNs, and PoPs.
- Act on both the real network state and the server response data to improve the current and future application experience.
- Recommend the fewest, most cost-efficient locations for your application

The Citrix difference is the use of real-time internet awareness and ITM steering to immediately and dramatically improve user experience and to provide insights for future application delivery planning.

your users originate and, based on their location, make recommendations for the best locations to put your content to help you meet your SLAs for application response should your traffic increase in certain geographies.

Always protecting your applications and APIs

Nowhere is intent-based automation more necessary than to automatically protect cloud applications and APIs from the onslaught of cyber threats. The use of the internet by remote workers and mobile device users to access multi-site applications is creating far more vulnerabilities than SecOps can manually keep up with. And the traditional approach of using a mix of vendor and home-grown security tools often does not cover all attack vectors.

Citrix App Delivery and Security Service integrates comprehensive application protection, which includes web application firewall, bot management, and API protection. It provides a single dashboard to define high-level multi-vector protection, confirm security policies, and apply a consistent feature set across all application environments. An example of intent-based automation at work is enabling SecOps to configure SSL settings to achieve strong encryption between users and servers. Normally SecOps would verify the result by getting the A+ rating on the Qualys SSL Labs test, which is a manual process for each server that involves many steps and invariably leaves apps and data vulnerable to malware hiding in weak encryption.

With Citrix App Delivery and Security Service, SecOps can define its intent to employ the strongest SSL configuration (A+ in the Qualys SSL Labs test) at the click of a button and have all their ADCs configured appropriately. The service will automatically:

- Restrict the use of SSL protocols to the latest, most secure versions
- Set the correct cipher suites
- Ensure that the SSL key length is long enough to withstand brute-force attacks

As the parameters of the A+ certification change, the service will automatically update the parameters to ensure your apps are protected with the strongest SSL security.

Additionally, Citrix App Delivery and Security Service uses a single-pass architecture for improved security performance. Recent independent testing by The Tolly Group showed that single-pass architecture for security services minimizes latency to provide a better application response for an optimal user experience.

The Citrix App Delivery and Security Service architecture

A paradigm shift in application delivery would not be possible without the right architecture. Citrix App Delivery and Security Service architecture implements human principles of “intent driven,” “always learning,” “always adapting” and “always protecting.”

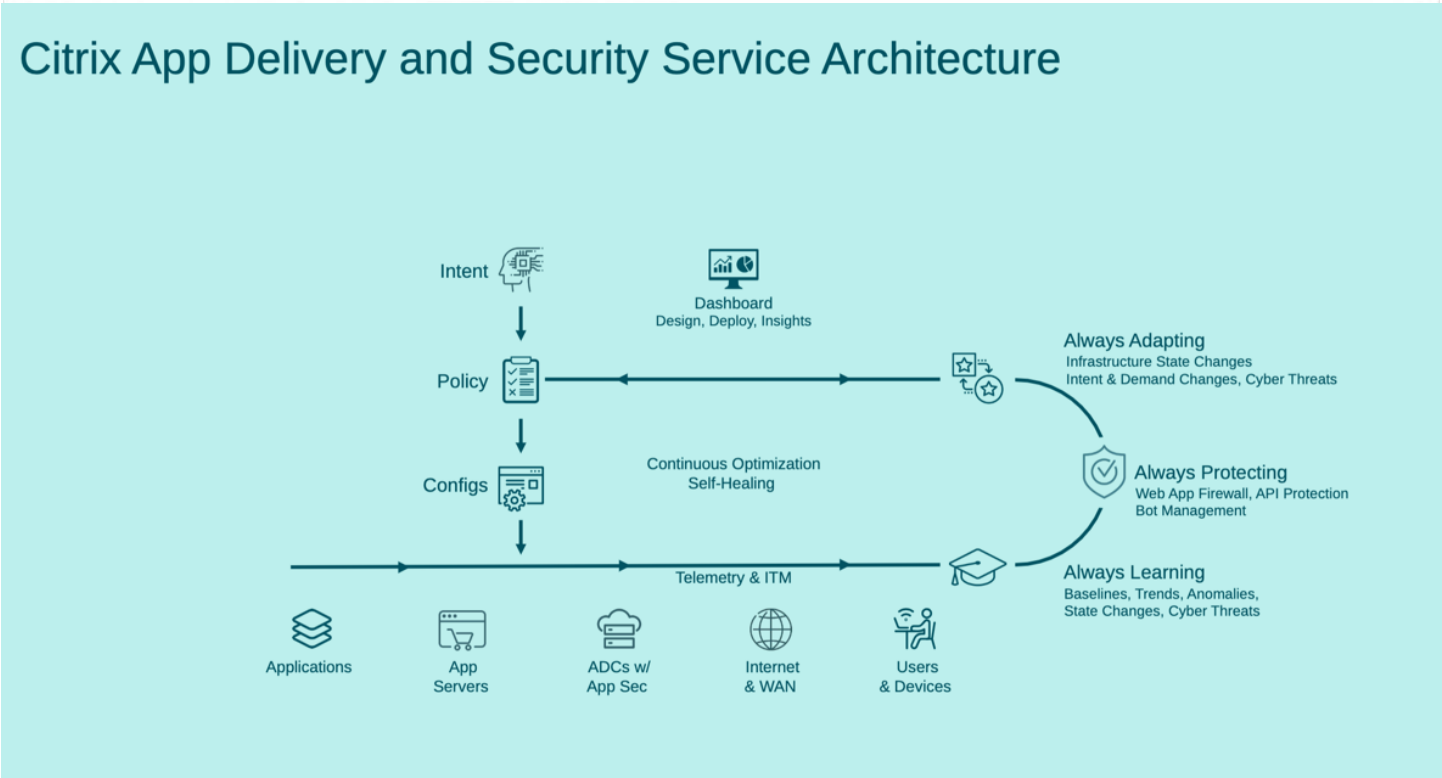
These principles ensure that the Citrix implementation will be robust for many years as IT teams undergo an automation transformation. To support the principles, the architecture uses four design attributes of its own:

1. Verifiable intent

Automatic translations from intent to policy, configurations, actions, and results are verifiable as they occur in the management dashboard.

2. Real-time visibility and analysis

- Continuous learning extracts actionable policy by interpreting internet-state telemetry and site telemetry such as



GSLB state, app state, and server state.

- It establishes baselines, such as “normal” latency between two geos. It distinguishes anomalies (unusual events) from trends (“new normal”).
- It operates in real time—that is, at the rate that events occur and that humans can view them, so that there is no significant lag until actions are taken.

3. Continuous optimization

- Policies continually enforce intent by triggering self-healing actions when an unusual event occurs, such as a user experiencing poor availability.
- Policy thresholds are updated using trends.

4. Hardened security isolation

- Citrix-managed PoPs cannot be taken offline inadvertently.
- The continuous optimization system cannot be easily hacked because telemetry and configurations are encrypted.

Getting started with the right solution

Citrix App Delivery and Security Service is available two ways: Citrix Managed and Self-Managed. Citrix Managed is the most advanced solution for apps hosted in the public cloud and comes with intent-based configuration and self-healing capabilities built in.

Citrix Managed

Designed for cloud native operations and journey to full automation from declarative intent

- Public cloud-based applications only
- Most advanced solution with intent-based automation, continuous optimization, and self-healing
- Internet-state awareness to provide an unparalleled user experience
- Analytics drive continuous improvement automatically
- Two simple billing meters—data processed and DNS queries¬—unlike public cloud providers that charge across multiple meters.
- Two editions: Advanced and Premium Editions with feature sets to fit the requirements of all our customers.

Self-Managed

Designed to provide the most flexible deployment options across on-premises and cloud

- On-premises and cloud applications managed the same way
- Analytics designed for IT staff interpretation and action
- Available in three editions: Standard, Advanced, and Premium.
- All the features and functionality included to support hybrid deployments, except for the intent-based, self-healing and internet-state awareness features. However, customers can try these capabilities for free because an entitlement of 100 TB per year is also included.

Conclusion

In the post-pandemic era, two trends dominate enterprise IT activities: ensuring a stellar application experience to differentiate the business with customers and accelerating the cloud transition for business applications that need to be accessible everywhere. But to achieve this, IT teams must squarely address three crucial decisions that will have far-reaching consequences:

1. How does IT address the complexity that comes with cloud deployments and operations?
2. How can IT ensure an optimal app experience globally over a dynamic internet with limited visibility?
3. How can IT protect applications, APIs, and data from the new vulnerabilities and advanced attacks that result from global-scale operations?

Citrix App Delivery and Security Service is a game changer in radically simple cloud-based application delivery and security. It uses an intent-based, self-healing, and internet-aware architecture built on four human principles, “intent based,” “always learning,” “always adapting” and “always protecting”:

- Intent based: Humans turn their intent into actions. When a person intends to take a holiday, they complete many different actions to make it happen by booking tickets, booking hotels, and more. Similarly, when IT defines the intent or KPIs for application delivery, Citrix App Delivery and Security Service will translate them into the appropriate policies and configuration to ensure the intent is met.
- Always learning: Just as humans are always learning about their environment and the changes that occur, Citrix App Delivery and Security Service is always learning about the application environment, the health of the servers, the state of the internet, new cyberthreats, and more.
- Always adapting: Humans use situational learning to continuously adapt, such as when a beginner golfer becomes a pro by repeatedly adjusting her technique as she learns from various situations. So too, does Citrix App Delivery and Security Service continuously optimize and self-heal to improve user experience and automatically reconfigures when application conditions change or performance degrades.
- Always protecting: Just as humans protect the things that are valuable to them, so does Citrix App Delivery and Security Service safeguard your business’s most valuable assets—applications and APIs—with a web application firewall, API protection, and bot management for comprehensive protection.

The use of these human principles enables awesome automation in delivering secure applications across hybrid and multi-cloud environments and are essential in the IT modernization journey.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States

©2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).