



ESG WHITE PAPER

Redefining Application Delivery and Security Services

Driving Simplicity, Agility, Security, and Performance with Intent-based Citrix App Delivery and Security Service

By Bob Laliberte, ESG Senior Analyst; and Leah Matuson, Research Analyst

September 2021

This ESG White Paper was commissioned by Citrix and is distributed under license from ESG.

Contents

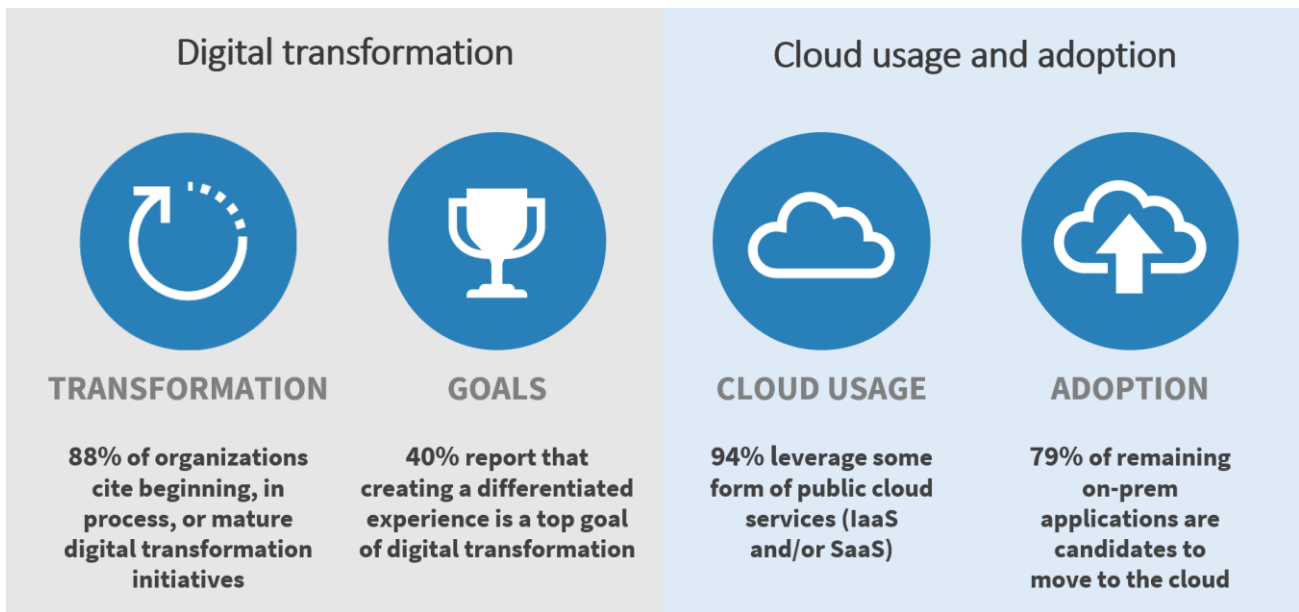
Modern IT and Application Environments Are Driving Change.....	3
Digital Transformation Also Creates Challenges	4
Negative Impact to Security	4
Challenges with Visibility and Performance.....	4
Manual Application Delivery Services Lifecycle	5
Citrix: Redefining the Delivery of Application and Security Services for Modern Environments	6
Citrix App Delivery and Security Service, an Innovative Solution Based on Four Key Principles	6
Agility.....	6
Security	7
Visibility.....	7
Automation	7
Citrix Application Delivery and Security Service Options.....	8
Citrix-Managed Service: Public Cloud	8
Self-Managed Service: Hybrid Cloud.....	8
The Bigger Truth	8

Modern IT and Application Environments Are Driving Change

Applications are essential to all industries—and the ability to swiftly develop and roll out new applications plays a critical part in ensuring an organization’s success. Consequently, to accommodate modern applications, organizations are transforming at a rapid rate. In fact, ESG research shows that digital transformation initiatives are accelerating, with 88% of organizations reporting that they have mature digital transformation initiatives, are beginning these initiatives, or have them in process.¹ Given an increasingly distributed IT environment, it should come as no surprise that operational efficiency is the most cited goal (56%) of digital transformation initiatives, while creating a differentiated customer experience (40%) is a top goal of digital transformation.

These digital transformations are also driving cloud adoption. A majority of organizations (94%) are leveraging public cloud services (IaaS and SaaS), with 78% reporting use of public cloud infrastructure (IaaS), up from just 17% a decade ago. In addition, more than three-quarters (79%) of on-premises applications and workloads are potential candidates to move to the cloud over the next five years (see Figure 1).

Figure 1. Digital Transformation and Cloud Services Acceleration



Source: Enterprise Strategy Group

Although many associate cloud-native applications with being deployed only in the public cloud, that is not the case. ESG research also shows that 70% of organizations plan to run cloud-native and container-based applications in hybrid environments, deploying these applications and workloads across private data centers, multiple public clouds, and edge locations.²

What’s more, a highly distributed application environment requires a modern, more comprehensive approach to security. According to ESG research, 47% of organizations report that strengthening cybersecurity is one of the considerations most

¹ Source: ESG Research Report, [2021 Technology Spending Intentions Survey](#), January 2021. All ESG research references and charts in this white paper have been taken from this research report, unless otherwise noted.

² Source: ESG Master Survey Results, [Trends in Modern Application Environments](#), December 2019.

important for justifying IT investments in 2021. And why not? Reliable application delivery and security services are critical to ensure the protection and performance of these modern applications—regardless of where they are located.

Digital Transformation Also Creates Challenges

While rapid transformation creates numerous opportunities, it also creates challenges for organizations across industries. There's no question that distributed environments are increasingly complex. According to ESG research, 75% of organizations surveyed believe that IT complexity has increased over the past two years, (up from 64% in 2020), with 21% of survey respondents citing that their IT environment is significantly more complex.

Many of the greatest drivers of complexity reported by ESG research respondents are related to new, more stringent security and privacy regulations, higher data volumes, and a burgeoning remote workforce due to COVID-19 work-from-home mandates—all presenting additional challenges to agility, security, network performance, and visibility.

Negative Impact to Security

Modern environments are designed to quickly change. By their very nature, these highly dynamic and distributed environments can often present significant challenges for security teams. In addition, finding skilled security resources is an ongoing problem, with 48% of ESG research respondents citing a problematic shortage of cybersecurity skills.

Also, with a highly distributed environment comes a much larger attack surface that needs to be protected. Organizations also struggle with the sheer number of security tools that require ongoing, manual correlation. Plus, organizations need to worry not just about securing the applications, but also all the APIs they use for communication and exchanging data.

Challenges with Visibility and Performance

There is no doubt that the distributed nature of modern environments can greatly impact an organization's network performance and visibility—but not in a positive way.

Troubleshooting efforts have become enormously difficult. The sheer size and scale of most modern IT environments has exceeded an organization's human capacity to effectively manage it. You can't

“You can't troubleshoot, much less manage, what you can't see.”

troubleshoot, much less manage, what you can't see. Hence, organizations are struggling to understand and maintain their increasingly complex distributed environments, while unable to have end-to-end visibility into their networks.

While many organizations may lack some visibility across their traditional corporate networks, they are increasingly leveraging the internet for their corporate connections. The lack of visibility across the internet only creates more challenges. Organizations deploying SD-WAN and home workers commonly leveraging broadband connections make the internet their de facto “corporate” network. While this allows for greater agility, it's an immense problem for corporate IT since they have no visibility into the internet. This can be problematic given varying latency across regions.

Because of this, poor application experiences can negatively impact employee satisfaction and productivity (especially for remote users) and also degrade the customer experience. Together, these factors can take an enormous toll on an organization's bottom line.

Manual Application Delivery Services Lifecycle



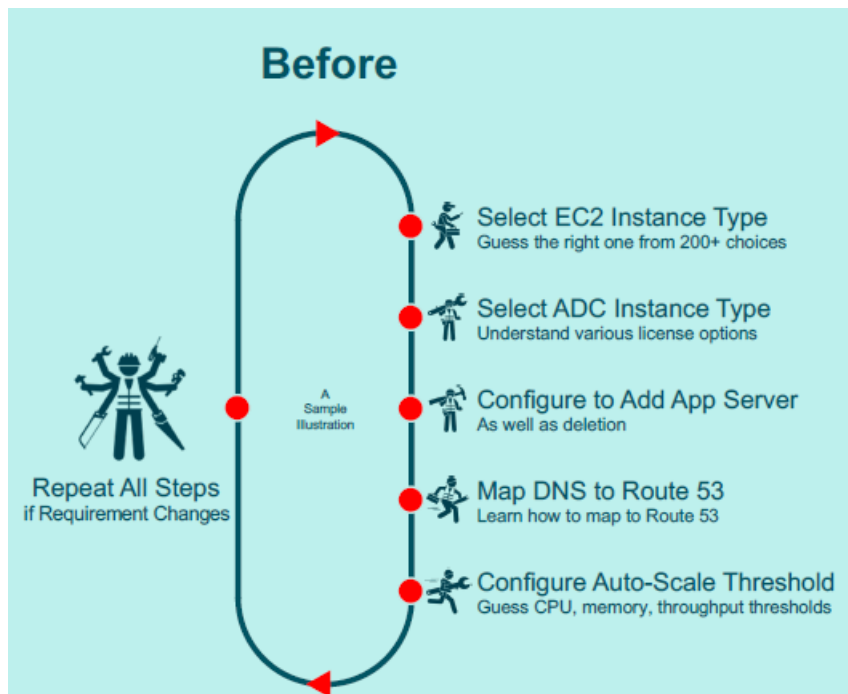
86%

Of organizations report being under pressure to launch new products and services

To maintain success and grow the bottom line, organizations must continue to evolve their application architecture in order to speed time to market. In fact, ESG research indicates that 86% of organizations believe they are under pressure to develop and launch new products and services at an accelerated pace.³

However, the process of delivering an application can still be a manual, time-consuming, and error-prone process—and *guessimates* are (unfortunately) commonplace (see Figure 2). From selecting and configuring the correct instances, to choosing the application delivery controller (ADC), to configuring the auto-scale thresholds, the current manual method is a hindrance to progress and the bottom line.

Figure 2. Typical Five-step Model of Manually Delivering an Application



Source: Citrix

In today’s digital economy, organizations must have a solution that provides reliable application delivery and security services, that is easy to manage, and that offers comprehensive visibility, while providing support for hybrid, multi-cloud, and cloud-native environments and the flexibility and agility necessary when dealing with an ever-changing modern application environment.

³ Source: ESG Master Survey Results, [Trends in Modern Application Environments](#), December 2019.

Citrix: Redefining the Delivery of Application and Security Services for Modern Environments

Citrix, a long-established leader in unified workspace, networking, and analytics solutions, has recognized the growing need to deliver reliable application delivery and security services for these modern environments and is bringing to market the Citrix App Delivery and Security Service. This comprehensive, intent-based application delivery and security services solution was designed for public cloud and hybrid cloud environments and offers Citrix-managed or self-managed options.

Citrix App Delivery and Security Service, an Innovative Solution Based on Four Key Principles

The Citrix App Delivery and Security Service is based on an intent-driven concept that incorporates the innate ability to translate intent into policy—and policy into orchestration—in order to automate and fast-track application deployment to simplify and speed application and API delivery and security.

Key tenets of the solution include:

- **Intent-based.** The solution translates intent, or KPIs, into actions based on the appropriate policies, and the policies then drive configurations.
- **Always Learning.** The solution is constantly learning about its environment (including the application layer, cyber-threat landscape, internet, servers, ADCs, and more) to automatically adjust services as needed.
- **Always Adapting.** The solution leverages closed-loop automation to drive self-healing and self-optimizing technology. With its ability to constantly verify changes, the solution can continuously improve application experience, performance, and security.
- **Always Protecting.** Leveraging multiple technologies like Web Application firewall, Bot management, and API protection, the solution ensures that applications and APIs are fully secured, connected, and protected.

Based on these key principles, Citrix App Delivery and Security Service offers a number of capabilities—which include agility, security, visibility, and automation—that provide a range of customer benefits.

Agility

Modern environments require highly agile solutions. With Citrix App Delivery and Security Service, intent is automatically translated into policy, which drives the orchestration engine. The solution enables IT and business to work together to ensure agility and performance by translating intent into action. For example, when IT defines intent or KPIs for application delivery, Citrix App Delivery and Security Service automatically translates this information into the appropriate policies and configurations.

This automated process enables organizations to:

- More quickly roll out new or updated applications.
- Leverage automation to reduce errors.
- Spend more time focusing on value-added business activities and less time on maintaining the status quo.

Security

Citrix App Delivery and Security Service helps organizations to maintain a consistent security posture, more easily meet compliance requirements, and enforce governance. The solution comprises Citrix Web App Firewall (WAF), bot management, and API protection, seamlessly integrating security to protect applications and APIs.

“Single pass architecture optimizes performance, with no tradeoff between performance and security.”

- Citrix WAF protects applications and APIs from known and unknown application attacks across public and hybrid cloud environments via a single code base across all ADC form factors to easily apply and enforce security policies.
- Citrix bot management helps identify, manage, and protect web applications from malicious bot attacks using real-time threat mitigation to neutralize automated basic and advanced attacks.
- Citrix single-pass architecture offers better performance and lower latency, which means there is no tradeoff between performance and security.

Visibility

Organizations can enhance the user experience by leveraging actionable internet-state visibility information to quickly mitigate any disruption to performance. Citrix Global Server Load Balancing (GSLB) included in the solution provides actionable internet-state visibility by leveraging Citrix Intelligent Traffic Management (ITM) technology to gain comprehensive insight into the internet.

Citrix has extensive visibility across 50,000 networks in 200+ countries, 1B sessions, and up to 10B data points per day. Thus, organizations are able to leverage this knowledge to provide optimal user experiences.

Armed with this information, IT has the potential to reduce latency significantly. Citrix enables IT to remove the guesswork about where to host application services by providing simulated scenarios to enhance the user experience (and company investment) *before* deployment. Hence, decisions are based on empirical (latency) data powered by Citrix ITM technology—and not guesstimates.

After initial deployment (day 2 and beyond), Citrix App Delivery and Security Service can also provide recommendations to help organizations accelerate the application hosting process, with cloud region automatically selected based on the lowest latency determination to the user’s ISP.

Automation

Given the typical manually intensive application delivery lifecycle, Citrix believes that its automated, intent-based service can improve operational efficiency by up to 60%. Automating previously manual tasks enables organizations to roll out new applications and update existing ones more quickly, eliminating the guesswork when it comes to ensuring performance and reducing waste (overprovisioned assets). Additionally, Citrix App Delivery and Security Service allows organizations to auto-select a PoP (or a server in that PoP) and provides the abilities to self-optimize for each user and to alert operations when they need to select a new site based on desired intent, such as lowest latency.

Citrix Application Delivery and Security Service Options

Citrix offers two options for deploying Citrix App Delivery and Security Service: Citrix-Managed Service or Self-Managed Service.

Citrix-Managed Service: Public Cloud

The Citrix-Managed Service for public cloud option encompasses intent-based and self-healing capabilities. Citrix-Managed Service is available in Advanced and Premium editions. Both editions can be deployed in AWS or Microsoft Azure and offer consumption-based pricing based on data processed and DNS queries.

Self-Managed Service: Hybrid Cloud

The Self-Managed Service option is a flexible solution for hybrid cloud use with central management capabilities. Organizations can leverage any Citrix ADC form factor to deploy the solution in on-premises data centers, public clouds, or edge locations. The Self-Managed Service option is a subscription service based on throughput and instances and is available in three editions: Standard, Advanced, and Premium. Note that intent-based and self-healing capabilities are not included in this option at this time.

The Bigger Truth

Organizations are rapidly transforming to support highly distributed modern application environments that are spread across multiple public clouds, private data centers, and edge locations. As these distributed environments grow more complex, organizations will require solutions that enable them to deliver reliable application and security services to ensure optimized availability, performance, and protection—regardless of user or application location.

Citrix is unveiling new, innovative services that enable organizations to not only regain control of these complex environments but to also empower them to accelerate deployments and leverage intent to drive automated healing, optimization, and learning. Citrix App Delivery and Security Service offers organizations a choice of two deployment options—either Citrix-Managed Service or Self-Managed Service.

By providing deep internet visibility tied to Citrix GSLB/ITM capabilities, Citrix harnesses billions of data points to ensure that applications are deployed at optimal locations for users (customers and employees), virtually guaranteeing peak performance and productivity. Plus, the solution's single-pass architecture allows multiple security tools to leverage data without impacting performance, while keeping applications and APIs secure.

Organizations looking to achieve higher levels of agility, security, visibility, and application experience would do well to explore how this intent-based, always learning, always adapting, always protecting Citrix App Delivery and Security Service could benefit their environment.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.



www.esg-global.com



contact@esg-global.com



508.482.0188