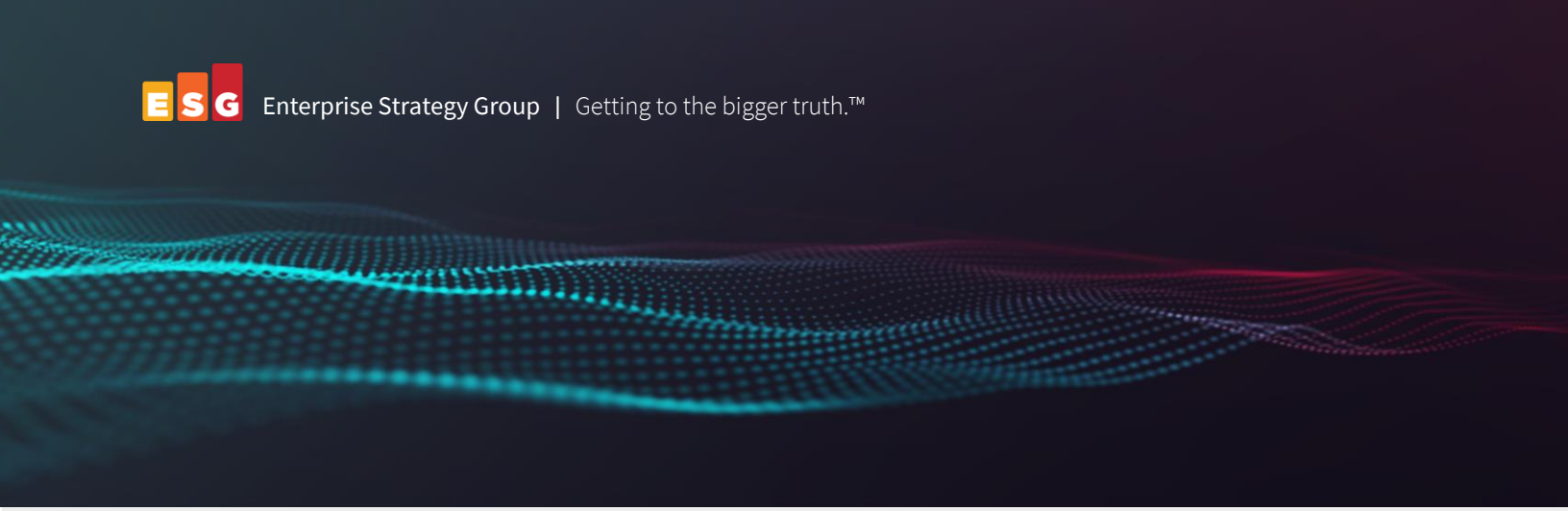


ESG WHITE PAPER

Citrix Application Delivery Management (ADM) Service

Driving Operational Efficiency and Visibility Across Distributed Environments (Hybrid, Multi-cloud, and Edge)

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

January 2021

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

Contents

Digital and Application Transformation Drive Progress Across Industries

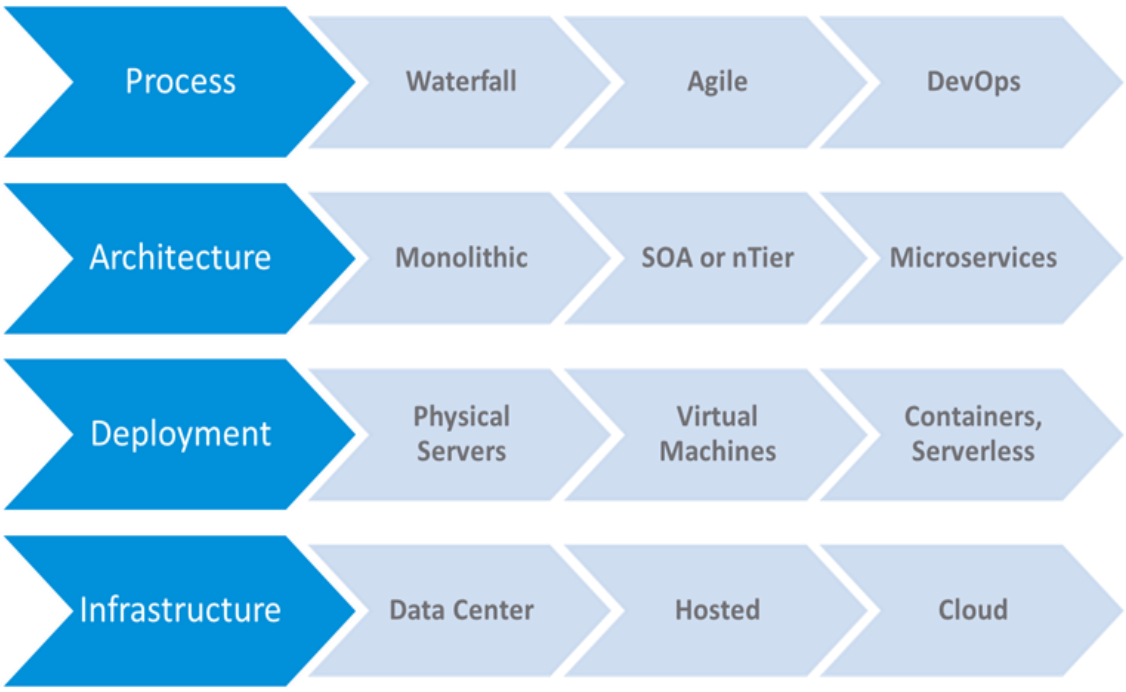
To gain a competitive edge, maintain success, and fuel the bottom line, increasing numbers of organizations continue to undergo digital transformation. According to ESG research, nearly three-quarters (72%) of respondents described their organization's digital transformation initiatives as mature (having implemented and optimized several initiatives) or in process (currently implementing and executing initiatives), up from 58% just a year ago.[1] What's more, ESG found the top goals of transformation include: increasing operational efficiency (56%); adopting tools and processes to allow users to interact and collaborate in new ways (49%); and creating a differentiated customer experience (40%).[2]

Application Architectures Are Evolving

Modern application architectures have evolved and are capable of delivering better customer experiences through faster development and upgrade capabilities. Previously, new monolithic-based applications could take years to develop and would be implemented on physical servers hosted in corporate data centers—and were only updated with a single major release and one or two minor releases per year.

Today, organizations are rapidly evolving their application architectures (see Figure 1). These modern applications leverage microservices-based architectures running on containers, enabling businesses to quickly bring new applications and services to market. In fact, ESG research validates the need to accelerate time to market, with a majority (86%) of organizations reporting that they are under pressure to deliver new products and services faster.[3]

Figure 1. The Evolution of Modern Applications



Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, December 2020.
[2] Ibid.
[3] Source: ESG Master Survey Results, *Trends in Modern Application Environments*, December 2019.

It is also interesting to note that there is a direct relationship between digital transformation maturity and the use of modern application architectures and methodologies. ESG research indicates that organizations with mature digital transformation initiatives are more than twice as likely (50% versus 22%) to prefer to use microservices architectures, and more than four times as likely (66% versus 14%) to use DevOps extensively, than those just beginning.[4] Keep in mind, many organizations will employ a mix of application types and environments, which is especially true for older, well-established companies.

Cloud and edge computing continue to gain traction and are key enablers of digital and application transformations. As part of digital transformation, organizations are rapidly adopting public cloud (IaaS), as well as distributing applications to the edge for real-time analytics. As such, application delivery services (application delivery controllers and management) are critical to ensure the security and performance of these applications—regardless of their architecture, underlying infrastructure, or location. As a result, these solutions need to ensure that they can enable transformation—and not impede it—especially when so many organizations are accelerating their digital transformation initiatives. This would include the ability to easily access management solutions from anywhere, which is especially important during this unprecedented time in which most employees are now working from home.

Transformation Also Creates Challenges

With all this change, comes multiple challenges—from a complicated hybrid IT infrastructure, to a burgeoning remote workforce, to escalating costs, to a swiftly evolving threat landscape.

Given the increasingly distributed nature of both IT and workers, it should come as no surprise that IT environments have grown increasingly complex. According to ESG research, 75% of organizations believe IT complexity has increased over the past two years (compared to 58% last year), with 21% citing IT as significantly more complex. The biggest drivers of IT complexity are the increase in remote workers due to COVID-19 work-from-home (WFH) mandates (49%), new data security and privacy regulations (38%), and higher volumes of data (38%).[5]

Distributed Applications Present Challenges

Cloud adoption is nearly ubiquitous, with 94% of organizations using public cloud services to some extent (IaaS or SaaS).[6] However, it is important to remember that cloud-native doesn't mean public cloud only. In fact, ESG research demonstrates that 70% of organizations running container-based applications plan to run them in a hybrid cloud environment, and 88% of organizations believe it will be important to manage modern applications across multiple public cloud environments.[7]

And how has the global pandemic affected organizations, especially their application strategies? ESG research shows that 24% of respondents stated that they expect the most significant impact of COVID-19 on their organization's longer-term business strategy to be the increased adoption of cloud applications, slightly trailing those who chose collaboration tools as the most significant impact of COVID (25%).[8]

As part of the highly distributed nature of IT, the edge is also gaining momentum. Fueled by the desire for real-time analytics at the edge, organizations are shifting applications to where data is created to eliminate the costly latency penalties associated with bringing the data to the analytics platform. Having said that, organizations are not building out

[4] Ibid.
[5] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, December 2020.
[6] Ibid.
[7] Source: ESG Master Survey Results, *Trends in Modern Application Environments*, December 2019.
[8] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, December 2020.

regional data centers but instead are deploying the minimal amount of infrastructure at the edge to support these real-time data analytics. But here's the conundrum— organizations must also recognize that performance and security are critical (and must be prepared to deliver secure and consistent application performance even at the edge).

Application Delivery Controller Challenges

Organizations leveraging application delivery controllers (ADC) to help with application performance and security need to overcome a number of challenges. Based on ESG research on trends in application delivery controllers,[9] organizations reported the following ADC challenges, which included:

- Cost of solutions (36%). As application environments have evolved, organizations have had to make new investments in their ADC environments, moving from hardware appliances to virtual machines and now to container-based form factors. In some cases, this also means moving to a new vendor for a certain environment, which drives up management costs.
- Inability to keep up with the changing cybersecurity threat landscape (24%). The cybersecurity threat landscape is continually evolving, and organizations are challenged to quickly deploy new policies across a highly distributed and possibly multi-vendor environment.
- Support for hybrid multi-cloud environments (24%). With modern application environments being distributed across on-premises and one or more public cloud environments, organizations struggle to deploy ADCs in these highly dynamic environments.
- Support for cloud-native environments (24%). As modern applications gain traction, ADCs need to extend support for their highly dynamic, ephemeral environments, while still supporting legacy applications. And as mentioned earlier, cloud-native environments can be deployed in both on-premises and public cloud environments.
- Lack of consistent management across on-premises and cloud environments (19%). One of the biggest challenges in these highly distributed environments is having visibility and centralized policy management (potentially even including closed loop automation) from a single pane of glass.

Unfortunately, assuring that remote workers have seamless access to the solutions necessary to perform their jobs is not so simple. Many remote workers have difficulty accessing on-premises solutions or are unable to access them at all (due to management resources being located outside the corporate network and corporate-controlled locations). While some organizations have begun returning employees to the brick-and-mortar office, a lasting impact of the pandemic will be a recognition that work is what you do—not where you do it—thus, organizations must ensure business resiliency and access to critical management solutions like their ADC environment, regardless of employee location.[10]

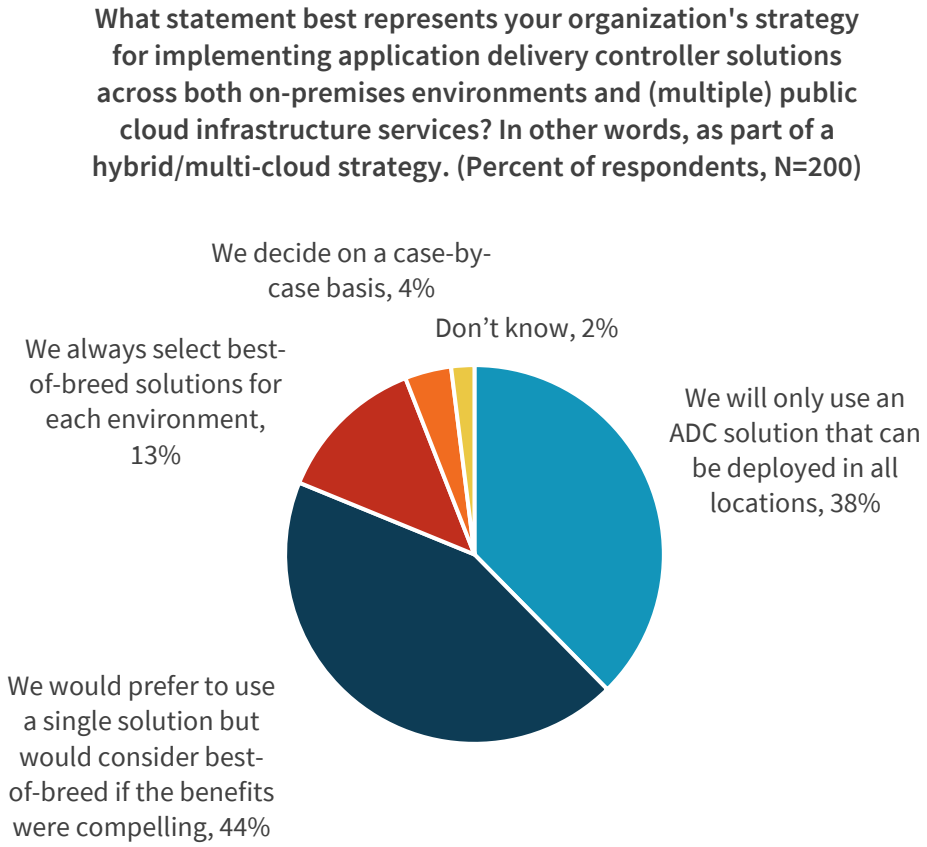
The Role of Modern Application Delivery Management (ADM) Solutions

With the countless challenges confronting organizations today, among the most pressing is how organizations can effectively manage a distributed cloud environment (i.e., hybrid, multi-cloud, and edge environments). This is especially true for application delivery controllers. As a result, ADC solutions need to evolve to not just meet the above-reported challenges but accelerate the transformation. To do so, they should:

[9] Source: ESG Master Survey Results, *Application Delivery Controller Trends*, August 2020.
[10] Source: ESG Research Report, *The Impact of the COVID-19 Pandemic on Remote Work, 2020 IT Spending, and Future Tech Strategies*, June 2020.

Leverage cloud-based controllers. By leveraging cloud-based application delivery controllers, organizations are able to more easily address their complex hybrid, multi-cloud, and edge environments. In fact, ESG research indicates that 38% will only use an ADC solution that can be deployed in all locations, while another 44% would prefer to use a single solution but would consider best of breed if the benefits were compelling (see Figure 2).[11] Cloud-based management enables organizations to gain greater visibility by leveraging a single management solution across a highly distributed environment (on-premises DC, public clouds, and edge locations).

Figure 2. Overall ADC Strategy for Distributed Environments



Source: Enterprise Strategy Group

For maximum effectiveness, modern cloud-based ADC management solutions must reduce complexity, be simple to use, and drive higher levels of operational efficiency. Cloud-based controllers eliminate manual, error-prone lifecycle management chores and don't require routine maintenance windows, thus decreasing the time required for manual updates, etc. Since all processes are performed in the cloud, valuable resources are freed up to focus on more strategic initiatives.

It should also be noted that certain industries (e.g., financial, government, healthcare, etc.) may be required to use on-premises ADC management—so while cloud-based is preferred, there should be an option to deploy on-premises as well.

Provide a consistent security posture across distributed cloud environments (i.e., hybrid, multi-public cloud, and edge). In a highly distributed environment, it can be difficult to ensure that every location has the most recent security patch or updated feature, especially if the updates need to be deployed manually. Even worse, not knowing there is an inconsistent

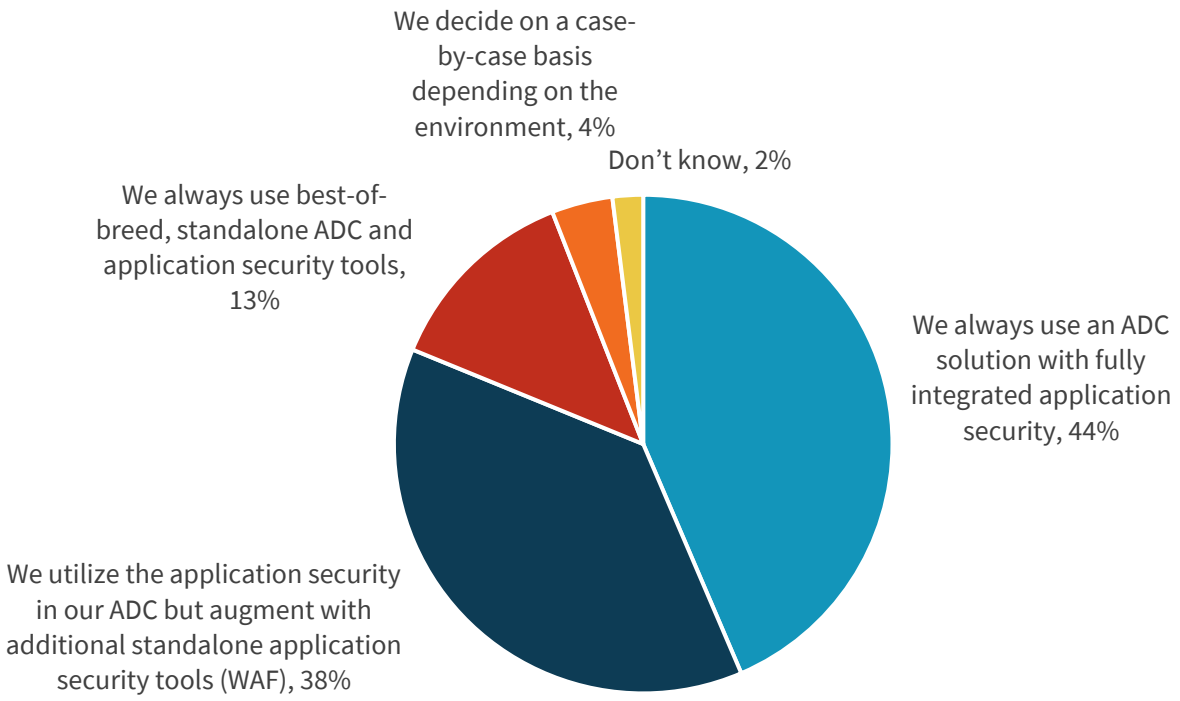
[11] Source: ESG Master Survey Results, *Application Delivery Controller Trends*, August 2020.

approach increases the threat of being breached. Thus, the ability to provide a consistent security posture across all distributed cloud environments is very important. Leveraging centralized management, organizations can easily create policies that are seamlessly enforced across distributed environments (i.e., when you create centralized policies in the cloud, these policies are automatically distributed to any locations where ADCs are found). This model is particularly effective when your ADCs also have integrated security functions and is a requirement for modern ADCs. This enables organizations to securely spin up new sites and ensure that existing ones are quickly and easily able to be updated with the latest security patches and functionality.

Based on ESG research, 44% of organizations always use an ADC with fully integrated application security, while another 38% utilize integrated application security in their ADC but augment that security with additional standalone application security tools such as web application firewalls (WAFs) (see Figure 3).[12]

Figure 3. ADC Security Strategy for Distributed Environments

What statement best represents your organization's strategy for implementing application security (e.g., web application firewall, DDoS, API protection, bot mitigation) with its application delivery controller environments? (Percent of respondents, N=200)



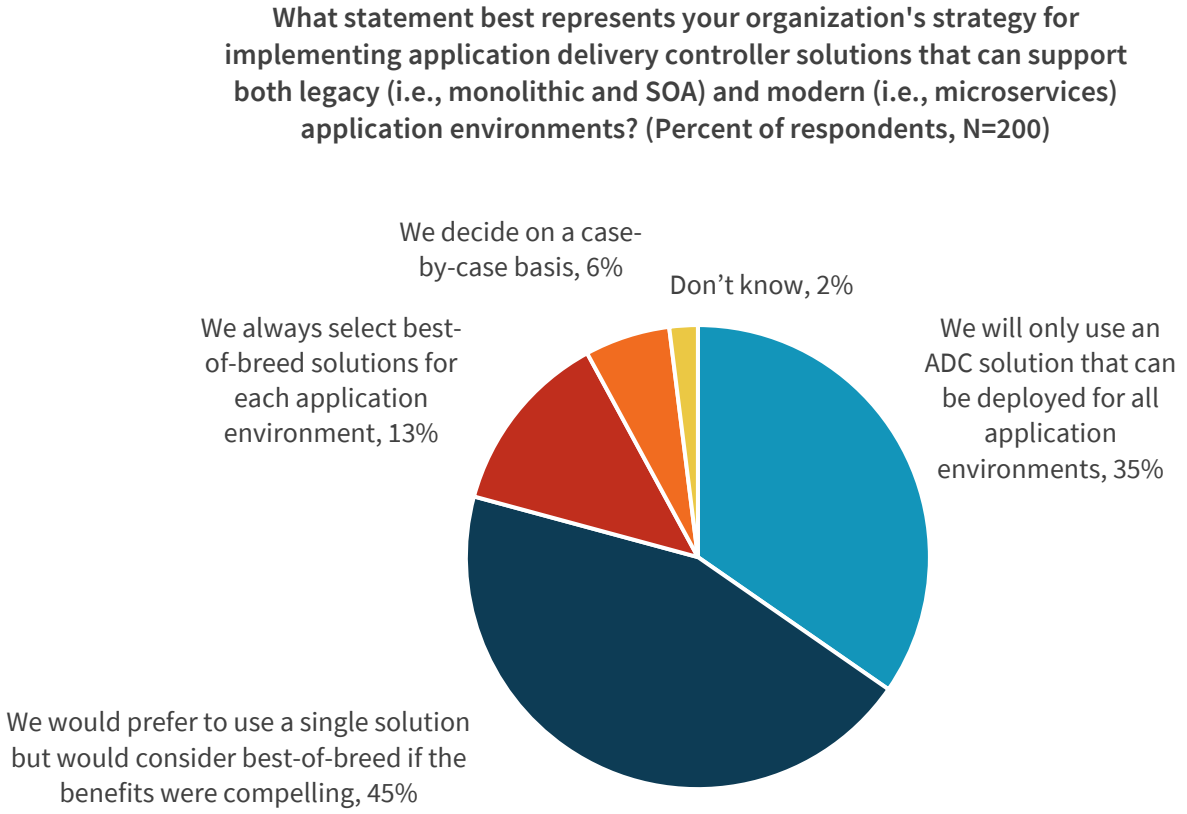
Source: Enterprise Strategy Group

Support heterogenous application environments. In general, more mature companies will possess a mix of legacy and modern applications. For operational efficiency and ease of migration, it is vital for organizations to select a single ADC portfolio that can address both legacy and modern applications. Based on ESG research, 35% of IT professionals said their organizations will only use an ADC solution that can be deployed for all application environments (monolithic to modern),

[12] Source: *ESG Master Survey Results, Application Delivery Controller Trends, August 2020.*

while another 45% said their organizations would prefer to use a single solution but would consider best of breed if the benefits were compelling (see Figure 4).[13]

Figure 4. ADC Strategy for Supporting Legacy and Modern Application Environments



Source: Enterprise Strategy Group

Leverage advanced artificial intelligence/machine learning (AI/ML) capabilities. Organizations should be able to take advantage of advanced intelligence capabilities to accelerate root cause analysis for faster problem resolution and anomaly detection to provide higher levels of security.

Predictive capacity planning is another area where organizations should consider leveraging the intelligence offered by AI/ML (e.g., organizations could use it to calculate when they will exhaust their capacity based on the rate at which they are currently scaling services. Ideally, solutions would be able to perform closed loop analysis, which would enable organizations to do things like automatically scale the environment when there is capacity available, which could be particularly useful in a public cloud environment.

Finally, this type of intelligence can be extremely useful when performing anomaly detection. With breaches to security becoming increasingly sophisticated, AI/ML enables the ADC to find anomalies that would otherwise go undetected, proactively alerting administrators.

Become more automated and operationally efficient. Automation is key to becoming more operationally efficient, streamlining deployments, and efficiently scaling ADC environments. Using automation helps to minimize the amount of time staff spends on repetitive manual tasks when deploying ADCs across a highly distributed environment. It would also

[13] Ibid.

minimize the time spent performing routine upgrades and patches (i.e., lifecycle management) for ADCs—both on-premises and in the cloud.

Automation can also accelerate troubleshooting activities, ideally leveraging closed loop self-healing capabilities. This would be essential in modern application environments that can change in a matter of just a few seconds. The system's ability to comprehend that there is a problem—and then automate corrective action—not only mitigates any potential risk of downtime, but also removes the need for staff involvement (i.e., taking valuable time to manually investigate, troubleshoot, and resolve a problem).

Utilize a flexible, consumption-based model. As organizations transition from a CapEx model to subscription-based or as-a-service models, it is also important to retain flexibility in licensing. Given that ADC cost was the top challenge reported by ESG research respondents, organizations need to leverage existing licenses supporting legacy environments as they transition to modern application architectures and not need to buy all new licenses. ESG research now indicates that four out of ten respondents would like to use a consumption-based model for ADCs.[14]

Provide cross-domain visibility and intelligent analytics across distributed environments. To gain valuable business insights, organizations must be able to employ intelligent, cross-domain analytics, where information about the infrastructure, applications, and security posture across the entire distributed environment (on-premises, public cloud, and edge environments) is collected and analyzed. To accomplish this, it will be imperative to have an ADC management solution that has complete end-to-end, cross-domain visibility.

Create role-based dashboards. Within an organization, there are multiple groups (Dev and IT Ops, application owners, security, etc.) that must be able to easily access information or spin up resources. A role-based dashboard offers organizations the capability to have the right people access the right data when they need it—enabling and extending visibility into distributed environments without adding potential security risks.

Citrix Application Delivery Management (ADM) Service

For more than 30 years, Citrix has been offering organizations server, application, desktop virtualization, networking, SaaS, and cloud solutions to enhance productivity and innovation. The vendor's unified workspace, networking, and analytics solutions help secure, manage, and monitor diverse technologies in complex, multifaceted distributed environments (on-premises, multi-cloud, and edge environments).

Citrix recently announced its Citrix Application Delivery Management (ADM) service. According to the vendor, Citrix ADM is an intuitive, cloud-based platform offering organizations an effective means to monitor, manage, orchestrate, and automate Citrix application delivery controller (ADC) instances, while troubleshooting the application delivery structure from a single, centralized, cloud-based console.

Citrix ADM service provides holistic, analytical insights and machine learning-based recommendations for the health, performance, and security of an organization's applications. With Citrix ADM, nothing needs to be installed or maintained. And because configuring ADCs is automated, organizations can be assured of timely updates and patches. In addition, automated scale on-demand enables organizations to save time and expense by only deploying resources when and where they are needed.

Citrix ADM service offers a number of capabilities, including the following:

[14] Source: ESG Master Survey Results, *Application Delivery Controller Trends*, August 2020.

A single pane of glass to provide a comprehensive view across a complex distributed environment

- The cloud-based controller offers a simple means to monitor an organization's entire application delivery infrastructure, including monoliths and microservices applications; and on-premises, public, private, and hybrid cloud environments; in any ADC form factor including physical, virtual, and cloud.
- Centralized control/Web-based access for remote IT workers. By providing this centralized visibility, Citrix ADM can enable organizations to eliminate finger pointing and drive greater operational efficiencies among ITOps, DevOps, and AppDev teams.
- Secure, role-based dashboards enable organizations to break down operational silos and provide teams, specifically those working remotely, with seamless collaboration and interaction, improving the user experience, enhancing operational efficiency, and ensuring effective security by only allowing appropriate levels of access.
- For those organizations that have regulations that prohibit a cloud-based management solution, Citrix ADM can be deployed on-premises, when required.

Analytics across the organization help administrators visualize and assess the entire distributed environment

- *Infrastructure analytics*. This capability provides administrators with the ability to visualize and assess their entire distributed environment (i.e., hybrid, multi-public cloud, and edge). Employing a number of indicators, such as instance health, instance availability, resource consumption, configuration and capacity issues, critical events, etc., Citrix ADM then assigns a holistic score for each ADC. This score provides a quick view of the health of an organization's infrastructure, but also provides the ability to drill down for more granular information.

> ***"Analytics across the organization help administrators visualize and assess the entire distributed environment."***

- *Application analytics*. This is used to obtain a comprehensive health score for each application that can be easily viewed from the Citrix ADM service dashboard. Administrators can easily view real-time and historical data, deviations, and anomalies related to application health and usage. This insight enables effective troubleshooting of overloaded applications, difficult-to-solve intermittent availability issues, and any anomalous performance issues.
- *Security analytics*. Similar to the application analytics, security analytics designate every application with a safety index based on its security posture. IT can easily view the index from a single pane of glass. This also includes a threat index that identifies the severity of potential attacks. Insights derived from these security analytics will enable operations to quickly ID applications under attack, and provide details about the sources, frequency, and type of attack.

Advanced analytics (AI/ML) offer greater insights across a distributed environment

- Citrix has leveraged its extensive ADC experience and vast amounts of data collected over the years to create and refine its machine learning algorithms to provide the ability to accelerate troubleshooting and root cause analysis.
- These models also enable operations teams to take advantage of predictive modeling to refine capacity planning, ensuring sufficient advance warning to allocate additional capacities as part of a scheduled upgrade and not an emergency maintenance window.

- Citrix ADM AI/ML capabilities also play a significant role in security operations, next-generation Web App Firewalls, and bot management. Aggregate data helps train Citrix ADM machine learning models to detect a wide variety of attacks, including account takeovers, excess client connections, abnormally high upload or download numbers, large data transactions, and more. Because Citrix ADM service is cloud-delivered, the latest security features and detection capabilities are available the moment they are released, with no update installations necessary. Citrix security notification services will automatically and proactively provide alerts on any detected anomalies.

Centralized, consistent security across distributed cloud environments

- Leveraging the ADM service's centralized cloud-based portal, organizations can easily define security policies, such as web application firewall (WAF) rules, bot management, and API security policies, and enforce those policies across a highly distributed environment that spans both on-premises data centers, edge locations, and public clouds.

- By employing consistent security policies across these distributed environments, organizations are able to more effectively meet regulatory compliance and industry guidelines.

Simple, complete SSL certificate lifecycle management

- Managing the SSL certificate lifecycle is vital, but it can take a great deal of time and effort by multiple groups, including security, network, and applications administrators. SLL certificates must be current to ensure they comply with corporate policy and meet regulatory compliance. Out of date certificated can render data inaccessible, creating problems, both internally and externally.

- Fortunately, Citrix ADM streamlines the entire SSL certificate management process, simplifying the entire lifecycle from creation of Certificate Signing Request (CSR) and SSL certificates, to SSL certificate installation and monitoring, to negotiated transactions, and notifications about expiring/expired certificates, and then automatically updating.

Automation provides greater operational efficiencies

- The Citrix ADM Service leverages automation in a number of areas to ensure operations teams can work more quickly and efficiently. Those areas include:

    - Automatic onboarding of existing Citrix ADCs. Citrix ADM service will look for existing Citrix ADC instances across all locations and automatically register them. This will save significant time in onboarding large, distributed environments.

    - Simplified upgrade services and lifecycle management. The cloud-based controller can automate the ADC upgrade process, freeing up time and ensuring the latest firmware versions or security patches are installed.

    - Citrix ADM service's self-healing infrastructure. It can automatically identify, analyze, and help mitigate potential problems, increasing productivity by reducing time expended on troubleshooting (and allowing resources to focus on value-added initiatives).

    - Autoscale. Citrix ADM leverages automation to scale cloud-based instances when needed. This is ideal for organizations that need to ensure performance and customer experience and also experience unexpected spikes in demand.

Innovative subscription licensing model offers flexibility and predictability

- Citrix ADM service is conveniently offered in a subscription-based consumption model, providing financial flexibility and predictable yearly costs.
- To further accelerate and enable these transformations, Citrix enables organizations to pool all their existing ADC licenses (i.e., physical devices, virtual or cloud) for greater flexibility and better investment protection. This enables organizations going through a digital transformation initiative to transfer a physical license to a virtual or cloud license when needed. This allows organizations to create a single ADC platform based on Citrix technology and shift resources as needed and where needed.

The Bigger Truth

Transformation efforts continue to gain momentum in organizations of all sizes and industries. Digital transformation initiatives and the evolution to modern application environments are driving the adoption of highly distributed cloud environments (i.e., hybrid, multi-cloud, and edge). At the same time, these organizations are also contending with the impact of COVID-19, which has served to accelerate both of these transitions and create the additional challenge of a mostly remote workforce.

As a result, organizations require solutions that will enable them to accelerate their transformation efforts and accommodate remote workers. Additionally, ESG research tells us that these solutions also need to drive greater operational efficiencies and deliver better customer experiences by ensuring that applications are more performant, resilient, and secure.

When it comes to simplifying the management of the application delivery infrastructure across a highly distributed application environment, Citrix ADM service checks all the boxes. Citrix ADM enables organizations to fully support heterogeneous application environments, from monolithic to microservices, across a highly distributed environment, from on-premises data centers and edge locations to one or more public clouds. And by leveraging the cloud-based controller, it can help remote workers to work more efficiently from anywhere by leveraging centralized policy creation and management, advanced intelligence, analytics, and automation to secure and scale a highly performant application delivery environment.

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