



Market Insight Report Reprint

Citrix aims to automate ADC deployments in the cloud with App Delivery and Security Service

September 29 2021

by **Mike Fratto**

Automation is critical for enterprises employing DevOps. Microservice-enabled application architectures and DevOps are driving IT to automate the network, but doing so will take time. With the launch of its App Delivery and Security Service, Citrix is attempting to bring intent-based networking to application deployment and the management of its application delivery controller.

451 Research

S&P Global

Market Intelligence

This report, licensed to Citrix, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.

Introduction

In 451 Research's Voice of the Enterprise: DevOps, Workloads & Key Projects 2021 study, 34% of respondents indicated that infrastructure automation was important for their DevOps plans, followed by the use of public cloud providers (33%). Process automation came in at 32%. Automation is critical for enterprises employing DevOps. Microservice-enabled application architectures and DevOps are driving IT to automate the network, but doing so will take time (whether they do it themselves or choose to use a network automation suite) because IT must build up its staff's skills and experience. With the launch of its App Delivery and Security Service, Citrix is attempting to bring intent-based networking to application deployment and the management of its application delivery controller (ADC).

THE TAKE

Citrix's new App Delivery and Security Service will likely be welcomed by clients that want to reduce the operational overhead of deploying and managing ADCs over an application's lifecycle. If the efficacy of the machine learning algorithms and resulting automated product selection prove out, enterprises will be able to manage application resources much more effectively. The machine learning and internet performance analytics and recommendation engine should also help IT sort out the most effective way to deploy and optimize applications on a regional and global basis. These are the kinds of tools that will help enterprise IT be responsive to application demands in the era of cloud and DevOps. Citrix has an opportunity to stay ahead of competitors with this service, but it will have to keep a steady pace of research and development to stay ahead of feature demand, improve cloud integration, and provide guardrails to control costs and deployment volume.

Context

Citrix is often early to market with new features and capabilities for its ADC product, including the launch of its App Delivery and Security Service, which attempts to bring intent-based networking to application deployment and the management of its ADCs. The service is initially aimed at automating the deployment and management of ADCs used in cloud services. AWS and Azure environments will be supported initially, but Citrix plans to add GCP and private cloud.

'Intent-based,' in the IT/network context, is used as an abstraction where an enterprise IT stakeholder defines the application capacity, performance, and security goals and requirements for an application, and the 'service' does the rest. This includes selecting the appropriate number and size of ADC instances, deploying them into the cloud service, configuring the cloud service's networking and then publishing the application to DNS to start serving traffic. The service manages autoscaling using machine learning.

Products

The App Delivery and Security Service is a new service available in Citrix Cloud. The Citrix Managed version includes all of the intent-based, automation, continuous optimization and actionable internet state-awareness features. It employs an intent-based paradigm, where administrators state desired outcomes, such as application latency and uptime, and the service determines how many ADCs to bring online and what instance sizes to use. The service can be purchased in one-year increments and is metered by the amount of data processed and the amount of DNS queries.

The App Delivery and Security Service includes analysis and visualization of internet performance from its Intelligent Traffic Management technology for planning and modeling application performance based on current internet conditions. It also distributes traffic to the right application location based on internet conditions.

For example, it combines internet performance from cloud services with application performance data and lets IT model and simulate application performance based on application location, and can proactively recommend changes to the topology, such as moving an application from one region to another to improve performance. This should help enterprise IT better understand how location impacts performance, and gives them tools to better architect application deployments. In future releases, Citrix should consider closing the loop by allowing the service to automatically make the changes when customers have gained confidence in the accuracy of the analysis. Generally, Citrix should continue to add features designed to remove IT intervention, which customers can adopt when they are ready.

Overall, the App Delivery and Security Service is well positioned to reduce the complexity of ADC deployment and management for IT departments. Additionally, creating APIs that allow programmatic integration in support of the deployment of continuous integration/deployment will likely be welcome by DevOps shops.

Citrix's SD-WAN offers application detection and optimization based on network quality, destination, performance requirements and policy. It offers application steering, WAN optimization (such as protocol optimization and data deduplication), and support for optimizing Microsoft 365 applications, as well as virtual applications and desktops, from its own Workspace product.

Citrix's ADC product, once known as NetScaler, is a full-featured ADC that uses the same code base in physical, virtual, cloud, bare-metal and container formats. ADC is available in three editions. Standard offers basic load balancing, security and management. Advanced adds the most features, including the option for web application firewall, integration with enterprise authentication systems, and support for Citrix Gateway. Premium adds web application firewall, bot management, API protection and historical HDX reporting to the mix.

Application Delivery Management (ADM) is a management system for Citrix ADC, Gateway, Secure Web Gateway and SD-WAN, including full configuration, management and licensing. In addition to management, ADM offers system, network, and application performance analytics and graphs across the entire product estate, helping to simplify monitoring and troubleshooting. Citrix AI and ML is used to help process the data and raise actionable insight.

Strategy

Citrix tends to go to market with its networking software in support of its virtual desktop and applications software, Workspace, which accounted for 74% of its Q2 2021 revenue at \$599m. Citrix uses synergies between its products. In the case of SD-WAN, Workspace pulls through SD-WAN deals to a far greater degree than SD-WAN pulls through Workspace, but on its own, SD-WAN appears to be performing well. Citrix doesn't break out per-product revenue, but its App Delivery and Security business, which includes ADC, SD-WAN and its security products, accounted for 23% of Q2 2021 revenue at \$186m. Citrix's strategy of helping enterprises deliver secure and reliable remote desktop and applications to users regardless of location is well supported by its other business units. Additionally, it offers flexible licensing with perpetual, pooled and subscription models, depending on the product.

Competition

On the ADC front, Citrix's primary competitors are F5, the market leader by revenue and (arguably) mindshare, and A10 Networks, which has a compelling ADC and security product line. Smaller competitors like HAproxy, Kemp Technologies and Pulse Secure continue to nip at Citrix's heels. Citrix ADC's breadth of features is well matched against F5 and A10, but the latter two have more brand recognition with IT in the ADC and security realm. Many of the features that Citrix brought to market earlier than competitors, like flexible licensing and multiple deployment formats, have become table stakes. While Citrix Cloud brings an XaaS-like capability to its products, F5's acquisition of Cloud Native WAN vendor Volterra in January gave one of Citrix's strongest competitors a cloud managed connectivity service that it could sell to customers, in addition to infrastructure with which to host its own networking and security products.

The Citrix Cloud-delivered App Delivery and Security Service is a competitive counter to F5's Volterra acquisition, and VoltStack in particular. The App Delivery and Security Service operates independent of any particular WAN service, couples the ADCs with the application components, and automates customers' infrastructure in cloud services, enabling enterprises to quickly add and move applications regionally using their existing cloud accounts. Automating the regional selection and movement of applications based on application performance requirements and regional network behavior for customers could give Citrix a competitive advantage.

On the SD-WAN front, Citrix has a solid product offering, but the market has matured and become largely undifferentiated. Now tied to SASE (secure access service edge), SD-WAN has become a foundational technology to a full-featured branch secure remote access solution, rather than a branch WAN enhancement. Competitors like Cisco and VMware, which acquired their SD-WAN products and have integrated them into their portfolios, and Palo Alto Networks, which also bought its way into the market, have all established cloud-based connectivity and security services, making the space difficult to compete in effectively. Citrix offers a SASE solution with a holistic, cloud-delivered security stack (SWG, CASB, DLP, malware protection, sandboxing, zero-trust and more) through Citrix SIA integrated with Citrix SD-WAN for management, orchestration and analytics.

SWOT Analysis

<p>STRENGTHS</p> <p>Citrix has some solid synergies between its networking products and Workspace, which helps to pull through deals because it has a technical advantage with Workspace customers. The App Delivery and Security Service simplifies ADC deployment via extensive use of automation and provides valuable recommendations on how to improve performance.</p>	<p>WEAKNESSES</p> <p>Citrix's strengths contribute to its weaknesses. Not enough emphasis is made to promote and market its networking products to the enterprise independent of Workspace. The App Delivery and Security Service has some loops to close, such as setting intent-based limits on data consumption and supporting more application environments in the cloud and on-premises.</p>
<p>OPPORTUNITIES</p> <p>Citrix's ADC product is well positioned from a feature and license standpoint for use in container environments as a replacement for standard-issue ingress proxies. Citrix has opportunities to expand its partnerships with MSPs and integrators with its SD-WAN product.</p>	<p>THREATS</p> <p>More SD-WAN products are forming the basis of vendor SASE services, which is already a very crowded field and one that Citrix is not well known in. It could easily get drowned out by competitors. With ADC, the shift to microservices has changed the primary roles in purchasing ADCs from networking IT to developers, who are more likely to use what is already in the environment.</p>

CONTACTS

The Americas

+1 877 863 1306

market.intelligence@spglobal.com

Europe, Middle East & Africa

+44 20 7176 1234

market.intelligence@spglobal.com

Asia-Pacific

+852 2533 3565

market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

Copyright © 2021 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.