Product Overview

Citrix ADC at a Glance

The most comprehensive application delivery solution from on-premises to the cloud

What is Citrix ADC?

Application delivery controllers (ADCs) are purpose-built networking appliances whose function is to improve the performance, security, and resiliency of application delivery. Starting its life as a load balancer, Citrix ADC directed requests to and offloaded connection management from back-end resources to provide scalability and availability for applications. In response to customer demand, Citrix ADC added many functionalities to optimize and secure applications to become one of the most feature-rich application delivery controllers available.

Citrix ADC can be deployed alongside any type of application—monolithic and microservices-based—in any on-premises and/or cloud-based environment. The single, unified code base across all Citrix ADC platforms ensures operational consistency across hybrid multi-cloud environments. Because Citrix ADC is uniquely positioned to see every connection to and from an application, it can collate telemetry for processing by Citrix Application Delivery Management (ADM). Citrix ADM provides end-to-end actionable analytics and proactive troubleshooting across your entire multi-cloud environment through a single, centralized pane of glass.

Building a better user experience

Modern businesses rely on applications for everything they do, and the user experience for these applications is absolutely critical. A poor user experience can negatively impact productivity, and revenue can be lost if customers abandon an eCommerce site because it's slow. Worse still, they may never return, damaging your business' brand and reputation. It's important to ensure that your applications are delivered effectively and that they are engaging and responsive. Citrix ADC keeps your business-critical applications readily available, performing at their best, and always secure to ensure that your business' user experience is consistently top notch.

Accelerate the transition to multi-cloud

All Citrix ADC platforms are built on a single, unified code base, allowing for smooth operational consistency, flexible pooled capacity licensing, and a consistent security posture across all deployments from on-premises to the cloud. This also means that all Citrix ADC instances can be managed centrally through a single pane of glass, Citrix ADM.

Pooled Capacity Licensing

Citrix ADC is available with pooled capacity licensing options that provide the flexibility to accelerate your journey to multi-cloud. Generally, the Citrix ADC product line has three family editions: Standard Edition, Advanced Edition, and Premium Edition. The differences between these editions are highlighted in the Feature by Edition Matrix.

Citrix ADC is also available on the leading public cloud providers and can be licensed either directly from their respective marketplaces or by bringing your own license (BYOL). Citrix ADC also offers an Express license for VPX form factors for on-premises and cloud deployments that includes many of the features of the standard license for users looking to try Citrix ADC before purchasing.

Learn more about Citrix ADC product editions and licensing options to meet your business needs.

Pooled capacity on Citrix ADC is a unique benefit of the unified code base and allows for the sharing and portability of throughput capacity or instance licenses across different Citrix ADC instances and form factors. This means that capacity can be allocated as needed to meet growing demand, then deallocated and redistributed to other ADC instances later. Pooled capacity licensing can be easily and centrally managed via Citrix ADM.

Citrix ADC is also available in zero-capacity hardware platforms for an easier, cost-effective transition to cloud. Learn more about Citrix ADC zero-capacity appliances in the data sheet.

Feature Matrix

For the full feature by edition matrix of Citrix ADC, see the appendix.

Maintain a consistent security posture

Application security is the bedrock foundation of a business' security posture. If critical applications are compromised, then all of a business' sensitive data is at risk—which has dire implications for user privacy, brand reputation, and business survival. Security is best implemented in layers, and Citrix ADC provides powerful security functionality across the applications stack from Layer 2 to Layer 7.

Network security

At a basic level, by proxying application requests, Citrix ADC helps prevent back-end resources being exposed to bad actors. This is extended through access control lists, where you can set up lists of IP addresses to which you want to permit or deny access.

An alternate, automated way of doing this is via IP reputation filtering. IP reputation is an automatically updated database of IP addresses that are known to send unwanted requests. You can use this to block IP addresses with a bad reputation. Used in conjunction with other Citrix ADC security tools, IP reputation will afford your applications and users protection from known spammers, hackers, bots, compromised webservers, phishing proxies, and more.

Citrix ADC also mitigates DDoS attacks on your applications. In addition to simple SYN cookies to protect against Layer 4 flood attacks, Citrix ADC incorporates Surge Protection, Priority Queuing, and SureConnect features that help manage DoS attacks (as well as other types of high load). In addition, the HTTP DoS Protection feature targets DoS attacks against your web sites, sending challenges to suspected attackers and dropping connections if the clients do not respond appropriately.

SSL encryption and decryption

Because nearly all web traffic is encrypted, Citrix ADC includes full SSL encryption and decryption capabilities. The Citrix ADC appliance acts as an SSL proxy and offloads computationally intensive encryption from back-end servers while simplifying labor-intensive certificate management. With support for the latest protocols and cipher suites (including TLS 1.3 and ECC), Citrix ADC affords the most secure end-to-end application data transfer.

You have full control over all the SSL protocols, cipher suites, and key strengths and can configure them to fit your specific security requirements. SSL profiles further simplify encryption management as well. Instead of configuring the settings on each SSL entity, you can configure them in a profile and bind the profile to all the entities that the settings apply to. This makes SSL management across your entire fleet much simpler.

Citrix ADC can also be used as the decryption point for other content inspection devices. For example, you can decrypt incoming traffic before forwarding it to an IDS. This removes the burden of encryption from the device, which means you can use fewer or smaller devices for content inspection. Citrix ADC also supports chaining of multiple content inspection devices.

Remote access

The SSL capabilities of Citrix ADC extend to a full remote access solution that includes identity control, endpoint inspection, and encryption of data in transit.

Citrix ADC is equipped with a full suite of authentication, authorization, and auditing (AAA) functionality. With support for LDAP, RADIUS, SAML, TACACS+, client certificates, web, various OTPs (including an integrated OTP), and more, the AAA features allow you to implement access controls with the Citrix ADC instead of managing these controls separately for each application. Citrix ADC can also act as an ADFS proxy to provide a single sign on experience for users and, through the use of SAML, extend this SSO to SaaS applications. For added security, Citrix ADC offers nFactor authentication. With nFactor's flexible and extensible framework, it is possible to define variable authentication policies that can vary dependent on users' environments and prior inputs, providing true contextual access to applications.

Citrix ADC supports endpoint analysis and can scan users' machines as they attempt to access applications remotely. Scanning the OS, AV, or web browser version as well as more advanced items like the registry pre- or post-authentication enables you to identify and control access accordingly.

As the gateway of choice for Citrix environments, Citrix ADC acts as a proxy for ICA traffic, creating an air gap for remote users. Moreover, Citrix ADC can relay the results of EPA scans to the Citrix farm, enabling it to dynamically invoke granular control policies on user activity. This SmartAccess can dynamically disable ICA channels enabling you to, among other things, switch off Drive Mapping on non-corporate devices, disable printing when a user is not in the office, remove USB access, disable cut and paste functionality, and more. The ability to parse the ICA protocol means that enforcement of these policies can even be carried on the Citrix ADC itself. Citrix ADC also acts as an RDP Proxy and supports PCoIP for access to other virtual desktop environments.

In addition to proxy access, Citrix ADC provides full SSL VPN functionality for network access as well as clientless VPN, meaning users can use their web browser to access applications without installing any local plug-ins.

Application security

Because applications and APIs are critical to any modern business, they are quickly becoming the largest attack vector for bad actors. Citrix ADC provides comprehensive application protection with integrated bot management and web application firewall functionality.

Bots traffic accounts for 30% or more of traffic on the internet. Citrix ADC bot management can detect incoming bot traffic and mitigate bot attacks to protect your web applications. Citrix ADC is able to identify bad bots and protect you from advanced security attacks. To do this, Citrix ADC utilizes a variety of techniques to identify bot threats—IP address lists, dynamic IP reputation, signatures of known bots, device fingerprinting, and behavioral analysis. Once bot traffic is identified it can be dropped, rate limited, redirected to another resource, or challenged with a CAPTCHA. When combined, these techniques can spot and mitigate bot traffic to your site to protect it from attacks and alleviate excess demand on infrastructure resources.

The Citrix web app firewall prevents security breaches, data loss, and possible unauthorized modifications to websites that access sensitive information by filtering both requests and responses, examining them for evidence of malicious activity, and blocking those that exhibit it. The web app firewall operates a hybrid security model using signatures to efficiently detect known application attacks and positive security with application learning to defend against zero-day attacks. With Citrix web app firewall, it is easy to safeguard your applications against the OWASP top 10 security vulnerabilities (including SQL injection and cross-site scripting) as well as the more advanced, application-specific threats like cookie consistency and hijacking attacks. In addition to protecting web servers and web sites from unauthorized access and misuse, the web app firewall protects against security vulnerabilities in legacy CGI code or scripts, other web frameworks, web server software, and the underlying operating systems. The Citrix web app firewall integrates with many of the top application vulnerability scanners—Cenzic, Qualys, WhiteHat, and more—which means you can turn scan results into deployable policies with just a few clicks.

Citrix ADC extends application security to APIs through its enterprise-grade API Gateway functionality. The API communications are protected via Citrix ADC's authentication, authorization, auditing, rate limiting, content routing, rewriting, bot management, and web app firewall functionalities.

Gain actionable insights with centralized observability

Because of the unique position in the network at which Citrix ADC sits, it invariably sees all traffic to and from applications. This includes every request to every URL, all web transactions and their exact times, and any security-related actions. In addition to outputting logs to syslog servers and sending SNMP traps, the Citrix ADC collates telemetry for all applications across sites and sends it to Citrix Application Delivery Management (ADM), a single console for centralized management, actionable insights, and proactive troubleshooting through one pane of glass.

Application health and performance

With intuitive dashboards and application scoring, Citrix ADM provides an overall view of the health and performance of your applications, Citrix ADC instances, and application delivery infrastructure as a whole. This coverage extends to all monolithic and microservices-based applications regardless of where they are located, enabling you to spot and resolve any anomalies that may arise across your environment.

Through Citrix ADC telemetry, Citrix ADM Web Insight provides information about client-network latency and server response time as well as a wealth of information about the application access. You can view lists of the top accessed applications, any URLs accessed by clients, OS and browser details, applications with the most back-end errors, and more. This deep visibility helps with alerting and troubleshooting across your entire infrastructure.

In addition, Citrix ADM provides specific analytics for Citrix environments. HDX Insight provides end-to-end visibility of traffic to Citrix Virtual Apps and Desktops. It offers real-time client and network latency metrics, historical reports, end-to-end performance data, and enables you easily troubleshoot performance issues.

Security analytics

With security analytics, you can assess the security status of your applications to determine their vulnerabilities and evaluate how well they are protected. Citrix ADM makes it easy to see the types and volume of attacks launched against your applications and their points of origin. It will also notify you of which applications are most at risk so that you can prioritize remediation appropriately.

Citrix ADM also tracks every SSL transaction and provides visibility into HTTPS transactions.

It offers both real-time and historic analysis of the different SSL protocols used, the ciphers and key lengths negotiated, the certificate types and sizes, as well as any SSL errors that may have occurred.

With the powerful security analytics of Gateway Insight, you're able to see failed login attempts and their causes. You can also view the number of applications launched, total and active sessions, and total bandwidth consumed by the applications. Drill down into details on the users, sessions, bandwidth, and launch errors for any application to facilitate easier troubleshooting for user authentication and usage issues.

Machine learning

Generally speaking, it is possible to trigger alerts when previously defined thresholds are met, but in many cases, it can be difficult to know an application's characteristics beforehand. Citrix ADM uses advanced machine learning techniques to overcome this challenge.

Citrix ADM calculates baselines for activity and failures for an application, then alerts you when there are notable deviations. This extends to different areas of Citrix ADM analytics. For example, Citrix ADM can monitor server response time by collating all server response times to determine acceptable levels automatically. Server responses slower than the baseline will trigger alerts.

A more complex example is using machine learning for security analytics to detect sophisticated attacks. In this case it is possible, based on client behavior, to detect an HTTP Slow Loris attack or even an account takeover attack. Both of these attack types can be comprised of legitimate actions that would not typically be detected by logs, but with machine learning analysis, the nefarious nature becomes apparent and these attacks can be mitigated.

Learn more about Citrix Application Delivery Management.

Optimize application delivery

Optimizing delivery of applications can improve the user experience and ensure that customers stay on your site and feel compelled to return. The Citrix ADC optimization features reduce transaction times between the clients and the servers, also reducing bandwidth consumption. They also enhance server performance by offloading some tasks and making others more efficient.

Caching

Optimization begins in the data center with the integrated caching functionality. Because Citrix ADC can store responses to client requests in memory, subsequent requests can be served from the ADC instead of being forwarded to the origin server. This not only accelerates the application response but also reduces the workload on the backend servers, which can cut infrastructure costs. This can be especially useful in cloud environments that charge you according to usage.

Compression

All modern browsers can accept compressed content. Citrix ADC has the ability to compress HTTP responses received from the servers and send them to browsers. This reduces the workload on the backend servers, and the smaller response sizes mean shorter download times and less bandwidth usage.

Front-end optimization

Citrix ADC also includes several front-end optimization techniques to reduce the number of required client requests, accelerate the responses, and improve the load and render times of application responses.

By utilizing domain sharding, Citrix ADC is able to overcome client connection limitations. This improves page rendering time by enabling client browsers to download more resources simultaneously.

In addition to HTTP compression, Citrix ADC can reduce the size of the HTML content sent to the client. By combining CSS files, removing whitespace within CSS or JavaScript, and converting GIF images to PNG, it is possible to improve page download and render times significantly. Similarly, placing the CSS, images, and JavaScript components in line with the HTML content reduces the number of requests made for content and also means that the page can be rendered more quickly. This is especially useful for mobile devices with limited cache sizes.

Image optimization

With Citrix ADC, it is possible to intelligently reduce the quality of images to improve download and render times. For example, mobile devices requesting high-resolution content can likely be served smaller versions instead. Of course, you are able to determine when and if this optimization is applied.

TCP optimization

There are several advanced TCP tuning and optimization techniques and capabilities built into Citrix ADC. These can be used to improve user experience and perceived download speeds significantly—especially when content is delivered across mobile networks. There are several TCP profiles built into the Citrix ADC (including BIC, CUBIC, Westwood, and Nile) which, when enabled, will adjust various TCP parameters. These parameters include window scaling, selective acknowledgement, maximum segment size, buffer size, and more to ensure that TCP communications are optimized.

Support for HTTP/2

To meet the trend of webpages serving more objects with larger sizes, Citrix ADC offers full support for HTTP/2. HTTP/2 is the latest iteration of the Hypertext Transfer Protocol (HTTP) and is designed to further enhance the user experience. Citrix ADC uses its capability to use the network connection more efficiently and reduces the number of requests required to retrieve content.

The overall goal of Citrix ADC optimizations is to utilize an array of various techniques and features which, when used together, significantly improve the user experience.

Ensure application availability and performance

Building a better user experience starts with availability and performance. After all, there is no experience if an application is not accessible or performing poorly. Citrix ADC has a variety of functionalities to ensure application resources are available and scale to meet growing user demand.

Load balancing

Load balancing enables an application to scale horizontally by adding more resources (servers) and distributing the load among them. Citrix ADC employs intelligent load balancing from Layer 2 to Layer 7. It can inspect incoming traffic and direct it based on multiple parameters across the network stack. In its simplest form, the IP addresses or TCP ports in a request can be used to make a decision about which server to send traffic to. Citrix ADC also supports content switching which allows traffic management decisions to be made based on L7 parameters. Information in the request headers enables traffic steering based on HTTP headers. For example, users can be routed to localized content based on their geographic location, mobile users can be directed to content appropriate for their device, and cookies can be used to specify content relevant to repeat visitors.

Citrix ADC uses a variety of algorithms to ensure traffic is distributed evenly. Simple round robin techniques will send requests to servers in turn, whereas techniques like least connections, lowest response time, and least packets account for back-end server conditions in the load balancing decision. Persistent connections can be assured using hashes of various parameters (IP address, TCP ports, etc.) or using cookies as previously mentioned. Cookie injection can be done by the Citrix ADC itself, removing the need to change application code unnecessarily.

While TCP load balancing can be applied to almost any protocol, Citrix ADC has a deep understanding and can parse several popular protocols (HTTP/S, Radius/Diameter, SIP, FIX, SIP, SQL, and more) which offers more granular control over applications and user experience.

Health monitoring

Intelligent health monitoring means that Citrix ADC will avoid sending requests to a server that is unable to respond. There are several built-in monitors to check on services and handle the most common protocols: PING, TCP, SSL, HTTP/S, FTP, LDAP, SNMP, SMTP, and many more. While these monitors can't be modified, Citrix ADC allows you to create custom monitors that can address complex conditions to suit your own specific applications.

GSLB

Local load balancing of applications components is important, but what happens if your entire data center or access to your public cloud is down? Citrix ADC Global Server Load Balancing (GSLB) is a feature that ensures that your user and customer requests are always received.

The Citrix ADC instances at each site communicate the state of their respective back-end resources and will direct requests to the site best able to respond. GSLB can be set to avoid requests being sent to a data center or cloud that is unavailable, or to send them to a data center or cloud that is closest to the user.

By leveraging load balancing and health monitoring together, Citrix ADC is able to keep applications available and performing their best wherever they are deployed.

Citrix ADC form factors

Virtual platforms

VPX

Citrix ADC VPX provides powerful web and application delivery features like load balancing, secure remote access, application acceleration, and consistent security, all in a simple, easy-to-install virtual appliance. Deploy Citrix ADC VPX on one of many supported industry-standard hypervisors—on demand—anywhere in the data center.

Citrix ADC is also easy to deploy as a virtual platform across private and public cloud environments with support for AWS, Microsoft Azure, and Google Cloud Platform. Purchase licenses from the cloud marketplaces or simply bring your own.

CPX

Citrix ADC CPX is built from the same single Citrix ADC code base but packaged as a container for easy deployment and management through a variety of popular container management systems.

Manage east-west traffic between microservices-based applications with sophisticated load balancing, SSL offloading, and DDoS protection. Deliver exceptional performance with multi-core Citrix ADC CPX as an ingress device to handle north-south traffic for popular cluster management tools such as Kubernetes. In its containerized form factor, Citrix ADC CPX integrates smoothly into the Kubernetes environment and is an integral part of the Citrix cloud native solution.

Learn more about the Citrix cloud native solution.

BLX

Citrix ADC BLX extends powerful application delivery features to bare metal. Run Citrix ADC as a Linux process without a hypervisor or container overhead on the hardware of your choice.

Find technical specifications of all Citrix ADC virtual platforms in the data sheet.

Physical platforms

MPX & SDX

Citrix ADC MPX is a physical appliance that provides powerful hardware-based application delivery and load balancing with options for high performance web application security and SSL offload support.

Citrix ADC SDX introduces fully isolated multi-tenant support on a single appliance for application workloads and groups. Deploying multiple virtual instances of Citrix ADC on one hardware appliance allows for the consolidation of multiple load balancers and application rollout.

Find technical specifications of all Citrix ADC physical platforms in the data sheet.

FIPS platforms

Citrix ADC offers specific physical and virtual platforms with FIPS 140-2 compliance and certification to meet the strictest compliance mandates of high security businesses and organizations.

Learn more about Citrix ADC FIPS platforms in the data sheet.

Citrix ADC Feature by Edition Matrix

Feature	Premium Edition	Advanced Edition	Standard Edition	Citrix Gateway	Universal License[1]
Application Availability					
L4 load balancing & L7 content switching	●	●	●		
Microsoft SQL load balancing	●	●	●		
AppExpert rate controls	●	●	●		
IPv6 support	●	●	●		
Traffic domains	●	●	●		
Subscriber-aware traffic steering	●	●	●		
Global server load balancing (GSLB)	●	●	○		
Carrier-grade network address translation (CGNAT)	●	●			
Dynamic routing protocols	●	●			
Surge protection & Priority queuing	●	●			
TriScale clustering	●	●			
Application Acceleration					
Client & server TCP optimizations	●	●	●		
Cache redirection	●	●	●		
AppCompress	●	●	○		
AppCache	●	○			
Application Security					
L4 DoS defenses	●	●	●		
L7 DoS defenses	●	●	●		

Feature	Premium Edition	Advanced Edition	Standard Edition	Citrix Gateway	Universal License[1]
L7 rewrite & responder	●	●	●	●	
Citrix Gateway Connector for Exchange ActiveSync	●	●			
AAA for traffic management	●	●			
Citrix Web App Firewall (WAF)	●	○			
IP reputation	●	○			
nFactor authentication	●	●			
Content inspection	●	●			
SSL forward proxy	●				
Citrix Cloud Connector	●				
Front-end Optimization[2]					
Content layout	●	●			
Domain sharding	●	●			
Image optimization	●	●			
Style sheets & JavaScript optimization	●	●			
TCP Protocol Optimization					
Multi-path TCP	●	●	●		
BIC & Cubic TCP	●	●	●		
Simple Manageability					
Citrix Application Delivery Management (ADM)	●	●	●		
AppExpert visual policy builder	●	●	●		
Action analytics	●	●	●		
AppExpert service callouts, templates, & visualizers	●	●	●		

Feature	Premium Edition	Advanced Edition	Standard Edition	Citrix Gateway	Universal License[1]
Role-based & AAA administration	●	●	●		
Configuration wizards	●	●	●		
Native Citrix web interface	●	●			
Comtrade Management Pack for Citrix ADC	●				
Citrix Gateway					
Federated identity	●	●			
One URL/SSO using SAML 2.0	●	●			
Centralized policy management (SmartControl)	●				●
Stateless RDP proxy	●	●			●
Microsoft Intune support	●	●			
PCoIP support	●	●	●		●
Cluster for ICA proxy (striped)	●	●			
Monitor Citrix Virtual Apps & Desktops traffic (real-time)	●	●			
Monitor Citrix Virtual Apps & Desktops traffic (historical)	●				
Monitor Citrix Gateway traffic (real-time)	●	●			
Monitor Citrix Gateway traffic (historical)	●				
Broad client support for plugins	●	●	●	●	●
Customizable web portal	●	●	●	●	●
SSL VPN remote access	●	●	●	●	●
ICA proxy to Citrix Virtual Apps & Desktops	●	●	●	●	
Contextual policies for Citrix Virtual Apps & Desktops (SmartAccess)	●	●	●	●	●

Feature	Premium Edition	Advanced Edition	Standard Edition	Citrix Gateway	Universal License[1]
Endpoint analysis	●	●	●	●	●
Secure browser-only access (CVPN)	●	●	●	●	●
Always-on	●	●	●	●	●
Integration with Citrix StoreFront	●	●	●		●

● Standard ○ Optional

1. For Citrix ADC versions after 11.1, the Standard edition includes (500) Universal licenses, Enterprise or Advanced editions include (1000) Universal licenses, and there are no Universal license requirements with Platinum or Premium editions. For versions previous to Citrix ADC 11.1, the Standard and Enterprise editions include (5) Universal licenses, and the Platinum edition includes (100) Universal licenses.
2. An AppCache license is required for several front-end optimization features.

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