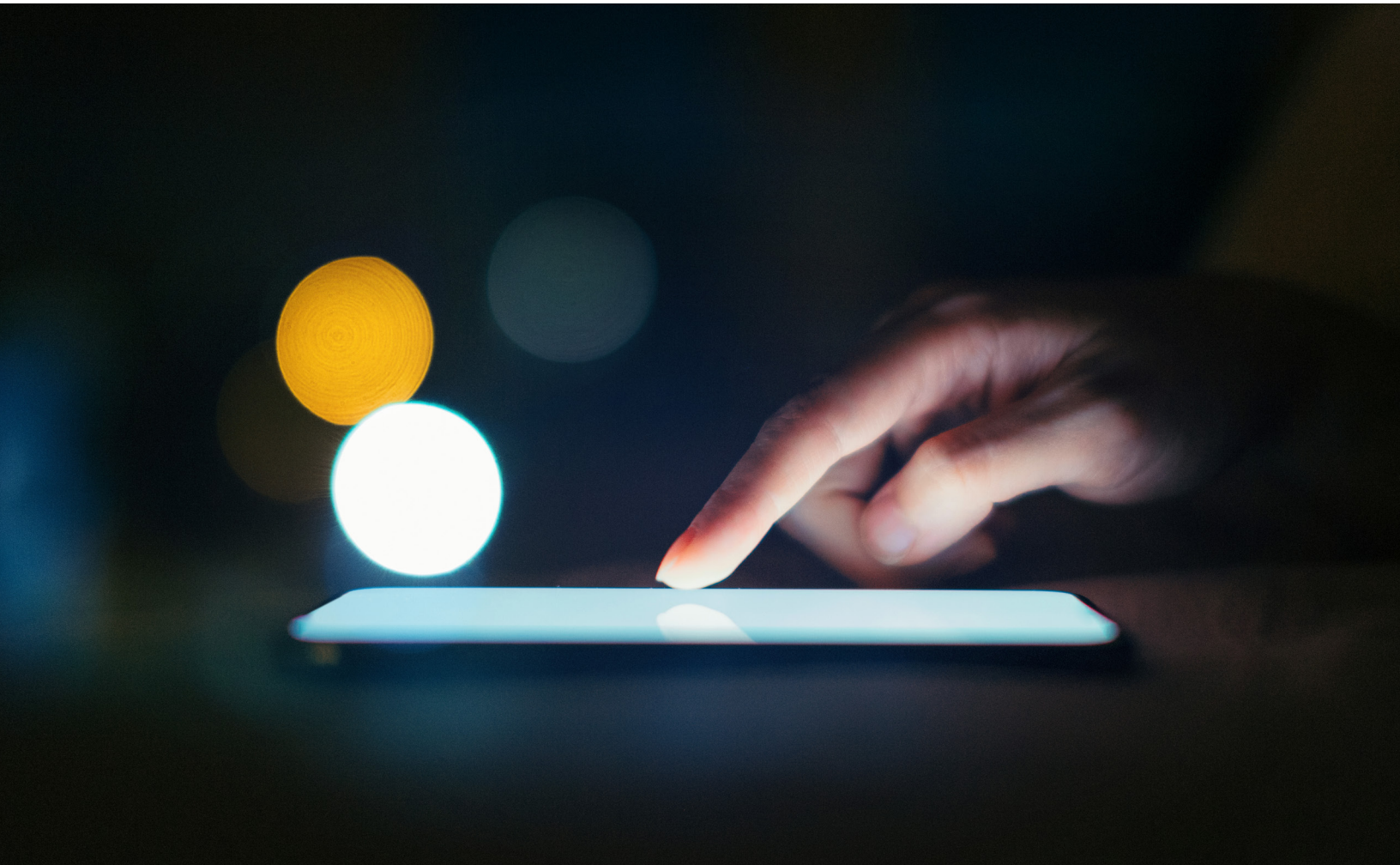
# Cisco Secure ADC Application Delivery Controller



© 2025 Cisco and/or its affiliates. All rights reserved.

# Contents


| | |
|---|---|
| The Application SLA Challenge | 3 |
| Legacy ADCs: Not Good Enough Anymore | 3 |
| High-Performance Application Delivery Platforms with Complete Layer 4-7 Feature Set | 5 |
| Engineered to Ensure Application Performance | 6 |
| Secure Application Delivery Services | 8 |
| Centralized Management and Automation | 9 |
| Secure ADC Platforms and Form Factors | 9 |
| Intuitive Licensing Packages | 10 |


© 2025 Cisco and/or its affiliates. All rights reserved.

**Cisco Secure Application Delivery Controller[1] (ADC) is the industry's only solution designed from the ground up to ensure predictable application Service-Level Agreements (SLAs) at all times. The only ADC packed with next-generation ADC services, Secure ADC cost-effectively addresses emerging IT challenges faced by enterprises and online businesses.**

## The Application SLA Challenge

In today's business landscape, IT is required to deliver consistent availability and performance-optimized user experiences for end users. Ongoing trends such as virtualization, consolidation, and cloud platforms are complicating these delivery requirements—the same resources are now shared by different applications and exposing organizations to SLA breaches. Moreover, cyberattacks that threaten application operations can potentially downgrade application SLAs. Finally, application infrastructure issues, including increased web application complexity and mobility, create additional challenges for delivering optimized application performance and meeting SLA requirements.

Whether it's an online web application, an internal mission-critical enterprise application such as CRM, ERP, or an organization's portal, end users expect to receive consistent quality of experience. The conclusion is clear: today's organizations require predictable application SLAs and require solutions to proactively monitor and manage application SLAs.

## Legacy ADCs: Not Good Enough Anymore

For years, companies have been using application delivery controllers (ADCs) to optimize the delivery of applications. However, the standard/legacy ADC is no longer adequate since application delivery is based on a best-effort approach. In a standard/legacy ADC, all resources are shared between server applications—there is no resource isolation per application and no resource reservation mechanism. This leads to SLA degradation of neighboring applications. Similarly, adding features or services to one application can degrade the overall ADC performance and impact the SLAs of other applications.

In addition, standard/legacy ADCs do not offer tools for monitoring application SLAs—they provide only acceleration features that mainly address the TCP/SSL layers but not the application, user, or device levels.

In contrast to legacy ADCs, a next-generation (NG) ADC provides real-user monitoring, best-in-class application-level acceleration features, and innovative security offerings. With full application SLA assurance, NG ADCs provide application-level resource reservation to allow for the addition of new services without performance penalties.

1 Secure ADC is manufactured by and sold by Radware as Alteon ADC. Cisco sells Alteon Application Delivery Controller (ADC), DDoS protection, and application and API protection solutions through its global OEM partnership with Radware.

© 2025 Cisco and/or its affiliates. All rights reserved.

## Complete Application SLA Assurance with Secure ADC

Cisco Secure ADC[1] (sold by Radware as Alteon ADC) is the industry's only ADC to ensure application SLAs at all times. Innovative and built from the ground up, it leverages next-generation services unavailable in other ADCs on the market. Secure ADC combines FastView® Web Performance Optimization (WPO), Application Performance Monitoring (APM), AppWall® Web Application Firewall (WAF), Authentication Gateway, Advanced Denial of Service (ADoS), and IT management (ITM)/bandwidth management, as well as industry-leading SSL performance with support for all the latest cyphers. Secure ADC/Alteon guarantees application SLAs several ways:

- Secure ADC is engineered to deliver full application-level resource isolation and is designed to prevent resources from maxing out.
- Secure ADC incorporates application performance management (APM) capabilities that provide full visibility into application SLAs, broken down by application, transaction, or location.
- The ADC integrates with FastView, the industry's most advanced WPO technology, which accelerates application responses for higher conversion rates, revenues, and productivity.
- Secure ADC is part of a unique attack mitigation architecture, allowing accurate detection and mitigation of the most advanced cyberattacks.
- Secure ADC provides industry-leading SSL acceleration performance, regardless of the model or form factor chosen, delivering the most cost-effective traffic encryption processing solution.

## Integrated Managed Application Protection

Application security, availability, and performance are critical for business. Secure ADC offers the most comprehensive, integrated managed application protection solution, designed to safeguard applications in any environment. Secure ADC delivers all the benefits of managed cloud application protection without the need to route traffic through the cloud. This solution is fully managed by experts, providing advanced and comprehensive protection without management overhead or bottlenecks, reducing TCO and setting a new standard in integrated app protection.

© 2025 Cisco and/or its affiliates. All rights reserved.

Secure ADC's integrated managed application protection, built on the proven Radware Cloud application protection service, leverages industry-leading web application firewall (WAF), API, bot, and threat intelligence technologies. Managed by experienced experts, it ensures rapid, comprehensive security for your applications, protecting against a wide range of threats while reducing management overhead.

Secure ADC application protection with SecurePath

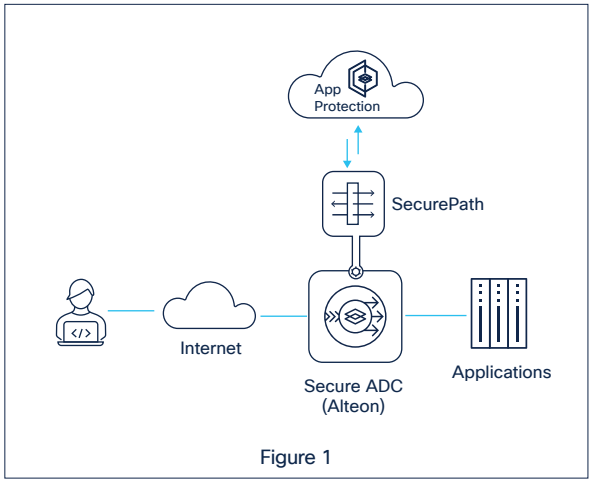



Figure 1

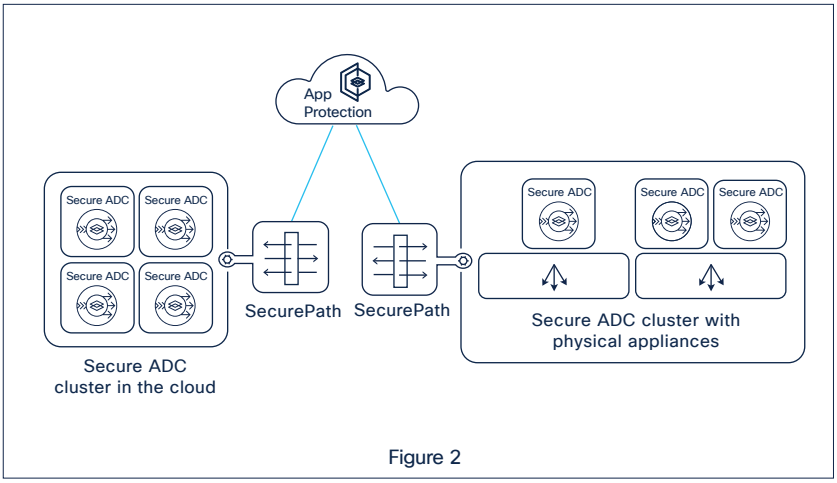



Figure 2

## High-Performance Application Delivery Platforms with Complete Layer 4-7 Feature Set

Secure ADC is a combination of hardware platforms and software, which deliver a rich set of application delivery capabilities with unmatched performance. It offers a complete set of Layer 4-7 services to ensure the availability, performance, and security of mission-critical applications in on-premises and cloud data centers. These extend to traffic redirection, content modification, persistency, redundancy, advanced health monitoring, and bandwidth management that optimize the delivery of mission-critical applications.

The ADC is designed to dynamically scale when necessary and without hardware modifications. It can scale on demand, adding more throughput, services, and virtual ADC (vADC) instances, or by leveraging an external, scalable resource pool (such as server infrastructure) for compute-intensive next-generation services. By eliminating the need to purchase additional ADC units, Secure ADC enables cost-effective hardware consolidation. It provides easy, quick provisioning of additional vADC instances, without service interruption, at a fraction of the cost of buying a physical ADC.

© 2025 Cisco and/or its affiliates. All rights reserved.

### Extended User-Defined ADC Functionality

AppShape®++ technology delivers scripting capabilities, allowing user-defined customization of the ADC service for specific application flow and scenario. By leveraging the script examples library, customers can use AppShape++ to refine various Layer 4-7 policies, including HTTP, HTTPS, TCP, User Datagram Protocol (UDP), SSL, and more—without application modifications, therefore reducing cost and risk.

## Engineered to Ensure Application Performance

Secure ADC's Perform package includes all the components required to ensure and enhance application performance. It provides a set of tools that enable the infrastructure and application teams to work together and proactively manage application performance.

### Guaranteed Resources per Application

Secure ADC enables companies to allocate a separate virtual ADC (vADC) instance per application, service, or department. Each vADC instance is fully isolated from neighboring instances and has independent resources such as CPU cores, memory, network stack, management control, and operating system versions. As a result, Secure ADC ensures complete fault isolation and predictable application SLA for delivered web applications at all times. In addition, next-generation services can be quickly and safely enabled without impacting the performance of other service applications.

### Full Application SLA Visibility with Application Performance Monitoring

The Secure ADC Application Performance Monitoring (APM) module provides real-time tracking of application SLAs by measuring user transactions, including errors. Embedded in the ADC, APM is an out-of-the-box solution that does not require synthetic transaction scripting or additional installation-reducing deployment time and costs. APM intuitively tracks SLA by location, user, application, and transaction type to expedite root cause analysis.

Additionally, APM provides historical reports based on user-defined SLAs that feature granular analysis, allowing the measurement of the delay per transaction phase and including data center time, network latency, and browser rendering time.

© 2025 Cisco and/or its affiliates. All rights reserved.

## Complete Toolset for Web Application Performance Acceleration

Secure ADC offers a complete set of tools for providing the highest application performance acceleration, including caching, compression, unmatched SSL offloading performance with all of the latest cyphers, and TCP optimization. Secure ADC enables faster communication between the client and server while offloading CPU-intensive tasks from the application server.

FastView technology, embedded in Secure ADC, adds a second layer of acceleration by providing up to 40% faster web application response times for a variety of end-user devices and browser types/versions and is optimized for mobile devices.

FastView automatically adapts to new application versions and new modules, which eliminates manual code optimization and allows organizations to focus on core business competence.

## HTTP/2

Secure ADC also offers an embedded HTTP/2 gateway, a third layer of acceleration that resolves many inherent HTTP 1.1 protocol performance bottlenecks, enabling additional acceleration of web applications. By leveraging the Secure ADC acceleration functionality and pairing it with FastView's content analysis algorithms, the HTTP/2 gateway automates server pushes, even before the client requests the content, and provides faster application response times.

Secure ADC offers a full set of acceleration tools that work in concert to deliver the fastest web application optimization experience for any type of browser, mobile device, or desktop device.

## Advanced Multi-Homing and Enterprise Gateway Capabilities

The integrated LinkProof® module delivers an application-aware, cost-effective solution to guarantee web application service levels and ensures internet connectivity at all times. By detecting application downtime through full- path application health monitoring, LinkProof NG allows organizations to pinpoint issues in various networking nodes and enables instant recovery along the entire WAN path.

By simultaneously load balancing and optimizing both inbound and outbound traffic of multiple WAN links, the solution serves as an advanced enterprise gateway that optimizes access to cloud applications by applying advanced TCP congestion control and selecting the best ISP link per service. LinkProof NG increases employee productivity and reduces operational costs at the branch office by supporting hybrid WAN architecture and aligning allocated WAN links by priority and accelerating employee access to software-as-a-service (SaaS) applications.

© 2025 Cisco and/or its affiliates. All rights reserved.

# Secure Application Delivery Services

The Secure services package includes a complete set of modules and functionalities that enable organizations to secure their applications. In addition, Secure ADC integrates with Radware's attack mitigation solutions, by leveraging a unique Defense Messaging mechanism that efficiently mitigates attacks by signaling attack information to Radware's DefensePipe® cloud service and DefensePro®, a data center attack mitigator located at the network perimeter.

## Simple and Safe Web Application Protection

The integration of advanced web application firewall (WAF) capabilities, such as a unique out-of-path WAF deployment mode and auto-policy generation features, enable risk-free implementation. In addition, full instance isolation and resource reservation ensures ADC resources. Even when WAF policies are updated, there is no impact on application availability and performance. This results in secured web application with guaranteed SLAs.

Finally, Secure ADC features a built-in authentication gateway that provides single sign-on (SSO) capabilities by supporting Radius, Active Directory, Lightweight Directory Access Protocol (LDAP), and RSA SecurID, and simplifies the user experience without compromising application security.

## Encrypted Traffic Interception and Inspection

Cisco Secure ADC natively provides the ability to offload inbound encrypted traffic decryption for inspection by security solutions such as next-generation firewalls, data leakage prevention systems, etc. To complete the solution, Secure ADC also offers a unique capability for intercepting outbound encrypted traffic as a forward proxy where the ADC does not own the SSL key, decrypt the content, and forward it in clear text to those same security servers.

The integrated URL classification engine enables Secure ADC to determine whether a specific transaction is considered private (e.g., browsing a bank account or healthcare site) and avoid intercepting the traffic for inspection—forwarding it to its destination untouched.

© 2025 Cisco and/or its affiliates. All rights reserved.

## Centralized Management and Automation

Secure ADC's centralized management system (APSolute Vision®) enables IT, security, and infrastructure managers to intuitively and collaboratively manage the entire solution portfolio, including all the Secure ADC devices, virtual ADC instances, and integrated modules such as AppWall and FastView. It also provides a performance monitoring and reporting tool that allows drill-down reports about user experience and the various elements in the application delivery chain. Using APSolute Vision also provides advanced automation tools to automatically execute management tasks across various Radware devices.

### Complete ADC Lifecycle Automation – Operator Toolbox

Operator Toolbox enables ADC experts and nonexperts to automate operational tasks. Operator Toolbox significantly reduces the operational workload (by up to 90%) throughout the ADC services' lifecycle, while minimizing human errors. Operator Toolbox allows any organization to customize its own automation tasks, per its specific application and work methodologies, designing wizards for different types of users (i.e., network admin or application developers, etc.) or providing for out-of-the-box wizards from a full library of certified scripts.

Deploying new and advanced application delivery services can literally be done through a few clicks of a button, requiring no ADC-specific experts in the process. Using APSolute Vision's centralized management system, administrators can create different script libraries with different user rights, tailored per the various user groups in the organization (i.e., application admins, application developers, network admin, etc.).

## Secure ADC Platforms and Form Factors

The Secure ADC solution includes a portfolio of physical appliances, virtual appliances, and cloud-based form factors, all sharing the same set of functionalities and modules, which guarantee application SLAs. On top of all other Layer 4-7 application delivery functions, performance optimization, and security functionality, the ADC delivers enhanced traffic encryption processing performance, which is available both via their optimized software and the latest hardware acceleration cards.

Secure ADC virtual appliances (vADC) and cloud appliances are no different, providing identical functionality as the physical Secure ADC appliances and industry-leading performance and traffic encryption capacities.

All Secure ADC appliances, starting at the entry level, support virtualization with a high density of virtual ADC instances per device, to enable any size organization to benefit from the cost savings associated with virtualization and ADC consolidation. The Secure ADC virtual appliance form factor is also available in a special version for DevOps teams, enabling instant deployment in any development environments and consumption of advanced ADC functionality via out-of-the-box wizards and automation scripts.

© 2025 Cisco and/or its affiliates. All rights reserved.

## Intuitive Licensing Packages

The new Secure ADC/Alteon D-line provides three different licensing packages to address different deployment scenarios and needs:

- The Deliver package for applications that require high-performance ADCs with advanced Layer 4-7 ADC functionality.
- The Perform package for deployment scenarios that require performance optimization, advanced application performance monitoring, and global server load balancing and link load balancing, as well as automated/optimized ADC service operation.
- The Secure package for applications that require the most advanced protection (with an embedded WAF module, authentication gateway) and for offloading SSL processing from perimeter security devices (with its emended SSL inspection module).

For more information about Cisco Secure ADC solutions, contact your Cisco sales representative today.

Alteon, AppWall, FastView, AppShape, LinkProof, DefensePipe, DefensePro, APSolute Vision are registered trademarks of Radware, Inc.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 03/25