

Securing Citrix

AEP White Paper

for Series A



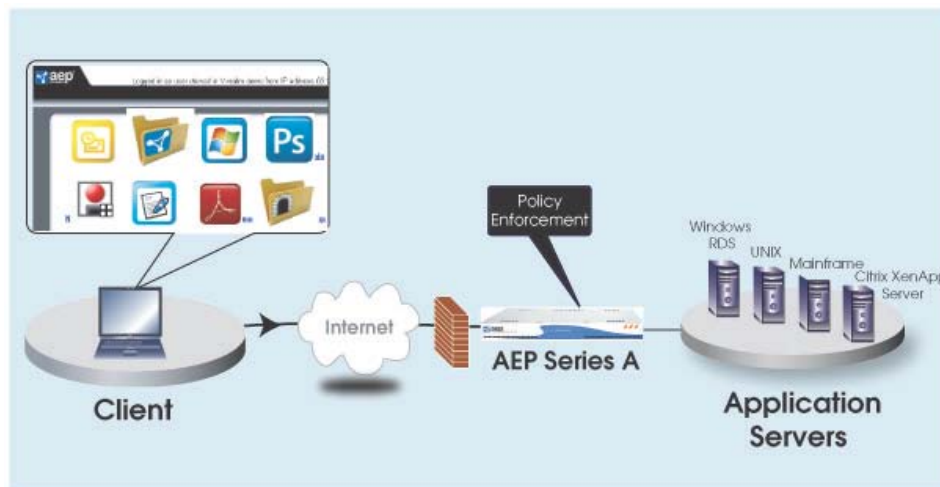
Securing Citrix with AEP Series A

Secure Delivery of Citrix & Other Applications in a Unified Solution

For years, Citrix® Systems has dominated the server-based computing market as the solution of choice for application access across the enterprise. Citrix XenApp (formerly Presentation Server) delivers a scalable, comprehensive solution that yields unequivocal dividends.

However, while Citrix Access Gateway (CAG) is designed for Citrix applications, it lacks support for the variety of applications typically required for business users. For many organizations, CAG does not represent a true enterprise-class remote access solution.

Series A offers a broader, more encompassing approach, providing crucial network security for XenApp – as well as other application environments – while adding important features unavailable with CAG. This paper describes the drawbacks associated with CAG and presents the AEP Series A Secure Application Access Gateway from AEP Networks, as the most versatile alternative for simple, secure access to Citrix XenApp and other application environments in a single hardware-based or virtual solution.



Series A Universal Application Access

Highly Secure. Built with security in mind, Series A includes extensive endpoint security, embedded 2-factor authentication server, session timeouts, robust reporting and logging, forced re-authentication, and client machine identification.

Series A provides this functionality through a powerful realms-based policy framework, allowing organizations to create customized policy enforcement “containers” depending on the access environment. For example, some users may require the full Outlook client via Citrix while others access Outlook Web Access through a reverse proxy. Road warriors who work from kiosks need endpoint integrity scans, while others must be limited to corporate-issued PCs only. A single Series A supports all of these requirements to suit the assorted access needs of the enterprise.



Universal Access to Many Application Types & Desktops

The types of applications users need to access and the environments in which they are hosted can vary and change over time. While today your data center may be a Citrix environment, using a completely flexible application access appliance future proofs your remote access solution and ensures an easier transition of data center changes.

With Series A, access to all of your business applications is delivered via a single appliance (virtual or hardware) ensuring efficient, all-inclusive access to mixed application server environments including Microsoft, Citrix, UNIX, Web-based and legacy (e.g., Mainframe). Users enjoy seamless access to all of their applications and are completely unaware of the multiple paths occurring behind the scenes.

In addition to authorized, individual applications, users can access their full desktops. Whether a physical desktop, virtual desktop or remote desktop services-driven desktops, Series A delivers custom-tailored access.

Why Pay a Premium to Deliver Non-Citrix Applications?

With AEP's Series A, you can deliver Citrix and Terminal services-based applications to users in a single solution for less. For instance, users who only need to access Outlook Web Access would not require a Citrix Access Gateway license reducing the concurrent user license cost by 70% (when comparing the cost of a Citrix XenApp Platinum license with a Series A user license).

All in One Webtop: Application and Desktop Access

Any or all of these mixed application types (Citrix, Windows RDS, Web-based applications, Mainframe, Desktop, SSL Tunnel) can be presented to a user in a unified, single web page with familiar icons representing each authorized application.

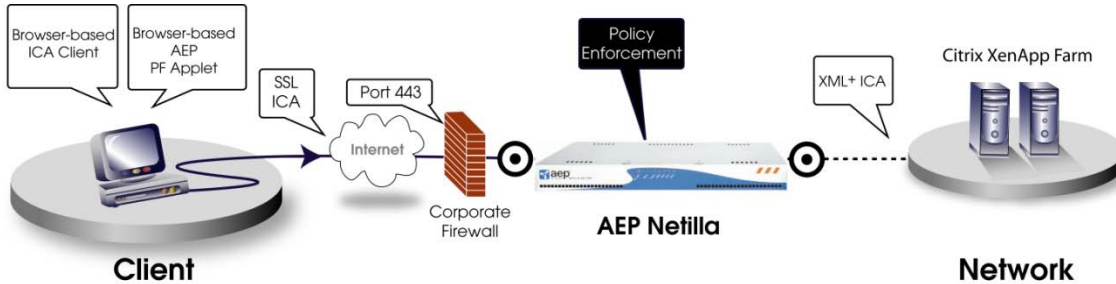
MyDesktop: Seamless Access to User Desktops

Series A's MyDesktop delivers automated direct access similar to GoToMyPC yet included within the product. Further, MyDesktop is delivered to users without using a Terminal Services session eliminating the need for a TSCAL.



How it Works: Securing XenApp Server Directly with AEP Series A

AEP Series A automatically delivers a Java client that sits on a remote Windows machine and looks for the TCP port that XenApp applications use. As soon as data starts to flow, the Port Forwarder Java client encapsulates and encrypts all the traffic in SSL and forwards it to the Series A appliance, where it can be deciphered and delivered to a Citrix XenApp server.



Series A ICA Client Push

Once the user logs in to Series A (via the authentication protocol used for the network), Series A pulls the authorized applications that have been defined on the Citrix servers, and publishes icons for these applications directly onto Series A's unified webtop. These Citrix icons are presented along with all the resources defined for that user (Web, Linux, mainframe or native Windows Terminal Server applications, as well as file shares). Alternatively, Series A can be configured to auto-launch Citrix applications directly from Series A's initial login screen. As an added benefit, updates made to Citrix applications are automatically reflected in the user's webtop, eliminating Administrator intervention.

When a Citrix application is requested by the end user (either via clicking an icon or via Series A's application auto-launch), Series A checks to see if an ICA client is already resident on the user's computer; if not, it will package a Java applet containing the Citrix ICA client (Java or ActiveX) – and install the client on the user's PC. Admin rights are not required for this process, nor are hosts file edits on the user's PC. This means that end users must only click an icon or log into the appliance to access Citrix applications; Series A provides the appropriate client seamlessly and without administrative hassles. Series A will publish any Citrix application – a Windows desktop, full program neighborhood, or single Citrix application – while standard Citrix printing and all other Presentation Server services such as Seamless Windows and load balancing are fully supported. And, you can control resource allocation for Citrix applications such as universal printing, audio resources, clipboard usage, drive mapping, and serial port redirection (all of which can be easily set to "on/off" as needed).

Of note: Series A provides access directly to the XenApp Servers themselves (without requiring Citrix Access Gateway), further cutting costs and management.



Easy to Deploy

From an administrator’s perspective, deploying XenApp via Series A is a single-admin screen process:

1. The Series A Admin enters the IP or Hostname of a Citrix server running the XML service OR the host/IP of the SSL Relay.
2. The Admin selects standard options (application icon to display, server address, default ICA client to deliver, etc.).
3. Admin selects users or groups (ActiveDirectory/LDAP) who are allowed to run the application set.

Comparing the Approaches

Citrix Access Gateway (CAG)	AEP Series A Secure Access Gateway
<ul style="list-style-type: none"> ▪ Access to “non Citrix” applications requires add ons 	<ul style="list-style-type: none"> ▪ Vendor independent: All Series A models support all types of applications and desktop access. No add ons.
<ul style="list-style-type: none"> ▪ Minimal endpoint security support 	<ul style="list-style-type: none"> ▪ Broad endpoint security support including cache cleaning, adaptive policies and host integrity checking (over 70 anti-virus & anti-spyware vendors supported).
<ul style="list-style-type: none"> ▪ Complex and costly high availability implementation. Simple active passive HA only available on CAG Enterprise edition. CAG Standard and Advanced require third party software and hardware for HA solution. 	<ul style="list-style-type: none"> ▪ HA available on all Series A hardware models. No additional software or hardware required.
<ul style="list-style-type: none"> ▪ No client machine identification. 	<ul style="list-style-type: none"> ▪ Provides “device fingerprinting”. Limits access to pre-approved client devices.
<ul style="list-style-type: none"> ▪ Complicated management and configuration 	<ul style="list-style-type: none"> ▪ Simple to deploy and manage: Single-screen setup
<ul style="list-style-type: none"> ▪ Complex for end users 	<ul style="list-style-type: none"> ▪ Citrix applications are published right in the user’s portal – one-click access to Citrix applications
<ul style="list-style-type: none"> ▪ Typical Citrix remote printing hassles 	<ul style="list-style-type: none"> ▪ Universal print driver for printing locally to ANY printer
<ul style="list-style-type: none"> ▪ Supports third-party 2-Factor only 	<ul style="list-style-type: none"> ▪ Integrated VASCO 2-Factor authentication server eliminates extra hardware purchase or Citrix infrastructure changes. Series A also supports all third-party 2-Factor solutions from RSA, Aladdin, and others.

Contact AEP Networks

sales@aepnetworks.com

www.aepnetworks.com