aep NETWORKS

Trusted Security Everywhere

# Security as a Service
# AEP **White Paper**
## for CloudProtect Remote

# Executive Summary

Everyone is talking about the Cloud.

Cloud computing is changing the way that businesses conduct their IT operations, bringing flexible processing, storage and applications to large and small organisations alike. For many, this new paradigm means all their IT is now run a service to be used and paid for on demand.

For the service provider (usually a Managed Service Provider, or MSP) cloud computing presents both an opportunity and a challenge:

> On the one hand the MSP can utilise all the benefits of cloud computing to deliver new services, attractively priced to match their customers' mode of use...
>
> On the other, the flexible dynamic nature of the virtual cloud environment presents a range of security challenges that cannot be addressed as if the cloud is a traditional, fixed environment.

MSP customers are looking for a subscription-based model for all their IT services. They already have ready access to infrastructure (IaaS), platforms (PaaS) and software (SaaS) as services, all offered on a pay as-you-use basis. Some of these services have elements of security built in, but for many the onus is on the customer to ensure adequate security.

**What if the MSP could offer Security as a Service (SECaaS)?**

At the moment, MSPs and their customers generally have to procure all additional security for the cloud on a traditional purchase basis. They incur large up-front costs to provide capacity that may never be used, invariably passing on these costs to their customers.

This paper explores the many benefits to an MSP of a new purchase model for security which is closely aligned to their existing service business. AEP's CloudProtect brings industry-leading Secure Application Access to MSPs with a pricing model that directly matches the way they sell SECaaS: they only pay for what they use as the use it.

With AEP's service model, the MSP enjoys a significantly better lifetime financial contribution, with no initial capital expenditure (CapEx). Moreover all risk of overcapacity and underutilisation is removed from the MSPs – their costs flex with their business. Equally, MSPs can scale immediately on demand – there is no wait to install new equipment or user licences. And finally, MSPs makes their own environmental contribution. In our simple model for a single MSP, the annual carbon saving equates to the carbon footprint of two domestic homes, or more than three private cars.

## Cloud Security

Security is a major concern with cloud computing, from service availability and reliability through to the protection of sensitive data and compliance issues. The customer's software and data are now physically outside the organisation, so security controls must be built into the cloud solution. But it is not that simple; security needs to be applied and administered differently in the cloud:

In the cloud, it's difficult to locate where data is physically stored. Physical and logical infrastructure is shared on a massive scale and users from companies with different trust levels often share the same resources.

Many security processes are buried in the cloud architecture, hidden behind layers of abstraction. The cloud is dynamic and transient, frequently changing to optimise performance, energy, availability and other service level objectives.

Service administration is largely automated, creating many opportunities for accidental or deliberate mis-configuration.

The cloud needs highly automated, virtualised security solutions, spanning the range of security domains from access control to authentication, encryption to intrusion detection.
Service providers have both a duty and an opportunity:

They must provide security at a level comparable to, or better than the levels that companies provide for themselves in traditional environments.

But they can deliver security as a service, at a scale commensurate with the user's needs, requiring little or no security device investment or maintenance by the user.

Cloud computing could actually make security more accessible, especially for smaller companies that struggle to implement effective countermeasures.

## Applying Cloud Security

MSPs usually implement their cloud security services by adding hardware appliances, much as they would in a traditional deployment. Where the cloud meets the physical network this may still be appropriate, but for many cloud security services a virtual solution is better. And while many security vendors now offer virtual appliances, the business model is still based very firmly on that of the traditional physical appliance.

MSPs who wish to offer Security as a Service (SECaaS) need a new security business paradigm— a service-based approach that matches their overall customer service model. Traditional modes of purchase are no longer suitable for their security infrastructure, with large up-front costs, fixed user licence fees and a heavy on-going maintenance burden. Instead, they need to move to a "Pay as You Use" service model, eliminating up-front capital expenditure (CapEx) and reducing their overall security spending.

# Secure Application Access

What is “Secure Application Access”? Broadly it means enabling users to reach virtually any business resource from anywhere at any time, with a level of access appropriate to the trust level of the user and security of the connection. Ideally, as we move to a service model, our service provider will offer our users the same service, policing access to the applications and data that they are providing on our behalf.

To be effective, the service itself must move to the cloud.

Successful application access control delivers:

**Broad Application Support –** Access to a mixed application environment such as Microsoft, Citrix, UNIX, Web and Mainframe applications and desktops.

**Seamless Authentication -** Plugs into existing authentication infrastructure, with support for common authentication mechanisms, such as Active Directory, LDAP and RADIUS.

**Network Security -** Encrypted tunnelling services with the same policy-based access to one or more types of access service.

**Client Security -** client health checks that validate the level and quality of client security measures such as anti-virus software, personal firewall, service packs and patches, together with deleting all traces of session data such as browser history and cookies.

**Unified Policy-Based Manaagement** - A single, common and simple way to manage users and provide controlled access to varied applications, significantly reducing management and operational costs.

## AEP Series A

As a trusted security vendor, AEP delivers a proven secure application access solution. AEP Series A is widely deployed around the world, securing access to mission critical resources for a broad range of customers. A comprehensive, approved product range, Series A comprises a range of physical and virtual appliances that meet all the key criteria for successful secure application access.

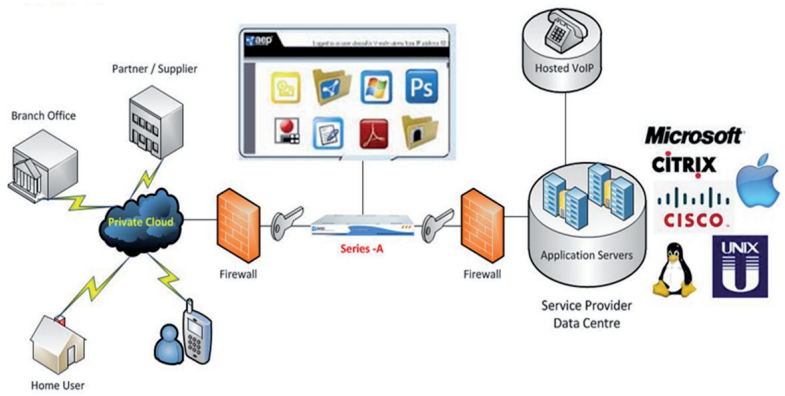


Figure 1 - Secure Application Access

Series A provides industry leading:

**Universal Application Support –** truly independent access to a range of applications from Microsoft and Citrix remote desktops to VDI, Web and legacy applications.

**Seamless Authentication -** supports most common authentication methods, including Active Directory, Novell NDS, LDAP, Open Directory, RADIUS, RSA SecurID, VASCO, PKI and HSPD-12.

**Network Security –** highly secure encrypted network access.

**Client Security –** comprehensive client health checks covering a broad range of client PC security measures.

**Unified Policy-Based Management –** Policy based user management using AEP V-Realms.

### Series A Virtual Edition

One of the first to implement a virtual access security appliance, AEP already has extensive experience deploying secure application access in a virtual environment. Series A VE is a pre-packaged virtual appliance which streamlines secure application access for virtual servers such as VMware ESX/ESXi, providing a comprehensive virtual solution.

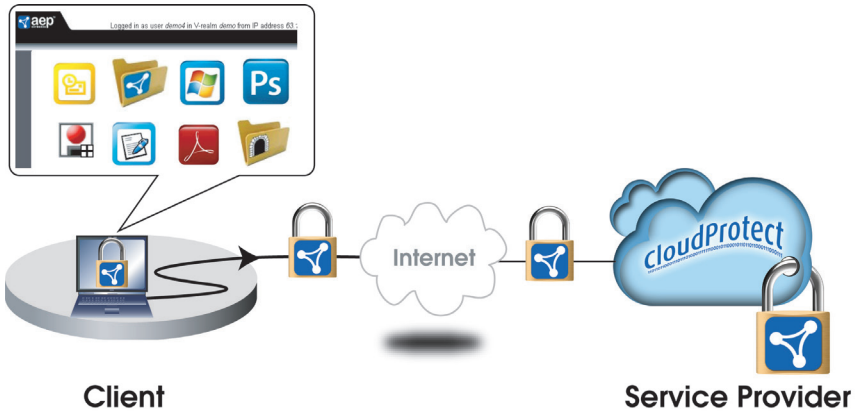


Figure 2- Series A VE

# CloudProtect

CloudProtect Application Security is a Security as a Service (SECaaS) offering that delivers highly secure, policy-based application and network access. It is a full feature version of AEP Series A VE specifically designed for MSPs delivering private cloud services to customers, enabling rapid deployment to match the flexible, elastic nature of the cloud, as shown in Figure 3.

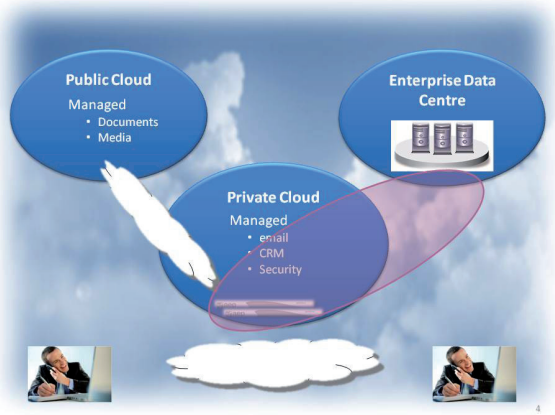


Figure 3 - CloudProtect Service

Offered as a virtual service, CloudProtect allows service providers to pay only for the application security they need, rather than purchasing traditional hardware and blocks of user licenses. Effectively, MSPs can now scale secure application access on demand, paying only when their customers request it and start using the service. Comprehensive user reports allow AEP to bill solely on usage – there are no hidden licensing or maintenance costs. Charged in arrears, on a Pay as You Go basis, CloudProtect allows MSPs to offer Secure Application Access as a SECaaS, fully aligned with their other cloud services. They can offer the service to new customers immediately and significantly, they can make a profit from these services from month one.

CloudProtect is:
**Highly Secure.** Delivers application, network, and client level security in one solution.
**Rapid.** Quick and easy to deploy and manage, enabling rapid service provisioning.
**Zero CapEx.** A true zero capital expenditure solution, with no dedicated hardware or licences to purchase up-front, just a "Pay as You Go" subscription-based charge.
**Highly Scalable.** Spin up CloudProtect virtual machines as needed and immediately meet growth demands without costly and time-consuming hardware deployments.
**Flexible.** CloudProtect is fully customisable. Embed it as the remote access component of the current cloud offering. Import reporting capabilities into the customer's control panel environment.
**Green.** No dedicated hardware. Save on power and cooling costs as well as rack space.
**Hypervisor Independent.** Seamless hypervisor integration including VMware ESX/ESXi, and Microsoft Hyper-V and Citrix XenServer.

CloudProtect supports a fully heterogeneous host and virtual desktop environment, including Microsoft, UNIX, Citrix, VDI, or the AEP MyDesktop Client Desktop Access. Equally, it provides full support to organisations looking to operate off open-source desktops.

With stringent endpoint policies, CloudProtect removes the danger of an unauthorised device connecting to the cloud environment. MSPs can assure their customers of the integrity of their sensitive data in the Public Cloud, as CloudProtect enables every device looking to access applications to be checked for full compliance with security standards.

## Financial Comparison

CloudProtect is priced to match the MSP business model. Crucially, as a subscription-based virtual service, there is no up-front capital expenditure (CapEx), enabling immediate revenue generation from customers while protecting the MSP against fluctuations in demand. The following scenario compares CloudProtect with traditional hardware and virtual appliance deployments.

Consider an MSP with five customers of different sizes requiring secure application access:

| Customer | Users Supported | Concurrent Users - Peak | Ave users per day |
|---|---|---|---|
| Customer 1 | 250 | 100 | 50 |
| Customer 2 | 1,000 | 250 | 100 |
| Customer 3 | 500 | 250 | 80 |
| Customer 4 | 10,000 | 2,500 | 800 |
| Customer 5 | 2,500 | 500 | 250 |
| **Total** | **14,250** | **3,600** | **1,280** |

Let us assume that each customer needs a separately managed appliance. In the traditional approach (for both hardware and virtual appliances) the ISV must decide the following for each customer:

**How many users must I provide for?**
This determines the size of hardware appliance or the number of virtual appliances.

**How many concurrent users must I support at peak operations?**
This determines the number of user licences to be purchased.

**What level of operating redundancy do I require in order to meet the service level agreement?**

**Do I require load balancing?**

These decisions determine the size (and cost) of the appliance(s). It is slightly simpler for virtual appliances — these are not usually sold by size, although they will have a user limit and multiple copies will need to be purchased for larger user numbers.

Hardware appliances will need to be procured, shipped and physically installed before the service can go operational. Again, the process with virtual appliances is more straightforward, but licences still need to be procured and enabled.

None of this applies to CloudProtect. The MSP simply downloads the virtual appliance, enables the user monitoring service with AEP and is ready to enrol users.

In our sample scenario, the costs to reach “go live” are:

| Deployment Option | Up-Front Costs |
|---|---|
| **CloudProtect** | € 0 |
| **Hardware Appliance** | € 292,500 |
| **Virtual Appliance** | € 227,500 |

Once the MSP is operating, further benefits of CloudProtect come to bear:

Users can be brought on-line as they need the service.

More importantly, the MSP only pays for the actual number of user connections (log-ins) each day. Traditionally, the MSP has had to guess (with the help of their customer) the peak user demand and then size accordingly.

With CloudProtect, if user access is low during weekends and holidays, that is all that is paid for; if it soars past the predicted peak at some stage, that level of usage is only billed for the day it occurs.

The MSP will be billing its customers as they use the service and being charged in exactly the same way, completely de-risking the provision of the service.

In the traditional model, if a large customer reduces its demand for the service in later years, the MSP may well be stuck with under-used equipment that it has already paid for. CloudProtect eliminates this risk as well.

Figure 4 shows the three-year cumulative contribution from the three secure application access solutions, CloudProtect, hardware appliance and virtual appliance.

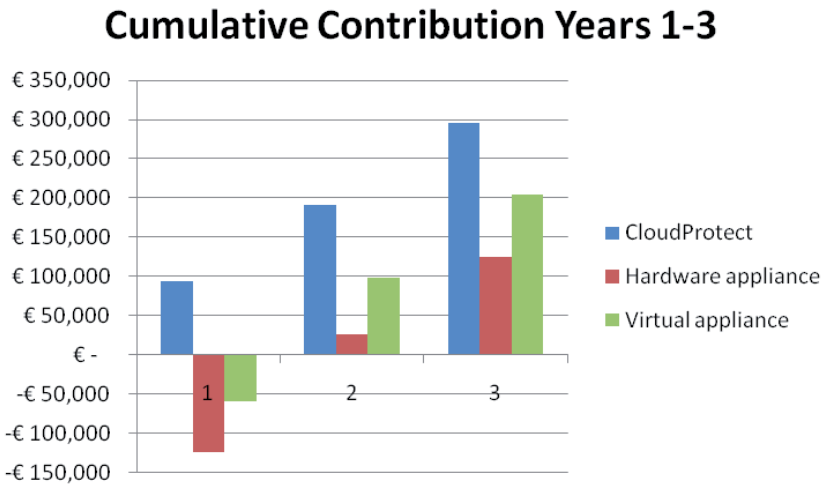


Figure 4 - Three Year Cumulative Contribution

**The example assumes:**

The MSP charges all customers on a per user connection basis, reducing its charges for higher volume connections.

The MSP's five customers remain on line over the three years.

Each customer agrees an initial peak concurrent user level with the MSP and charges are set accordingly. In the traditional model, if a customer grows beyond this level, the MSP must purchase additional user licences and potentially, hardware; the MSP may be able to negotiate a penalty if they drop below the agreed level, although this will be hard to apply in practice.

Different user growth rates are applied to different customers.

Actual daily usage is taken as a simple average and applied over 220 days per year— the typical number of work days, allowing for weekends, holidays and sickness. Sometimes usage may be at or above the peak concurrent level, at others, well below but this doesn't affect the quality of service that is delivered.

CloudProtect delivers a regular, predictable contribution from day one. Moreover, it continues to deliver better value to the MSP without risk, enabling them to focus on developing their business in line with their customer needs.

## Environmental Issues

Let us also compare the environmental costs of a virtual appliance with a hardware appliance in our model. For our five sample customers we require a total of 10 physical appliances, to provide for load scaling and fail-over. Both CloudProtect and the virtual appliance solution require no additional appliances. There may be a small incremental increase in load on the cloud infrastructure, but this is likely to be just a few percent of the equivalent appliance power. Using an industry average of 300W per appliance and assuming 24*7 operations, the incremental carbon footprint of the appliances is: **19 Tonnes CO2 per annum**. While for the datacentre this may only be an increment of a few percent, it is equivalent to the annual power consumed by two private homes or three to four private cars.

## Summary

In summary, let us look at the comparative benefits of CloudProtect with traditional hardware or virtual appliances. We have identified clear cost, deployment, management and environmental benefits against the hardware appliance. In addition, while the virtual appliance conveys the same deployment, management and environmental benefits to the MSP, the managed subscription pricing of CloudProtect still brings significant cost benefits. Table 1 compares the benefits of each approach.

| | CloudProtect Remote | CloudProtect Anytime | Traditional Appliance |
|---|---|---|---|
| **Application Access Security Features** | Full premium licence services* | Full premium licence services* | Full premium licence services* |
| **Physical Separation** | Not separated – security depends on security of virtual environment | Not separated – security depends on security of virtual environment | Separate device, but back-end connection still depends on security of virtual environment |
| **Ease of deployment** | Easy to deploy | Easy to deploy | Physical installation and network level deployment |
| **Ease of management in a virtual domain** | Matches virtual domain management | Matches virtual domain management | Constrains application access to a single physical network gateway |
| **Flexible customer charging** | Charged as used on a per user per day basis | Charged on lease basis | None. Charged on estimated concurrent users |
| **Up-front costs** | None | Minimised – depending on lease arrangements | Highest, hardware appliance and user software licenses |
| **Operating costs** | Varies directly with customer usage | Varies directly with registered user numbers | Fixed, but prone to spikes from new user demand |
| **Maintenance** | Included in subscription fee | Included in subscription fee | Charged annually, typically 15% to 20% of purchase price |
| **Carbon Footprint** | Minimal | Minimal | High |

*Includes SSL Tunnel Service, Web Application Access, Active Directory and LDAP, 2-factor Authentication, General Files Access, Citrix Terminal Services, Windows Terminal Services, MyDesktop, Client Integrity, Cache Cleaner, Client Machine ID, Virtual Realms, Multiple Home Pages, Virtual Desktop Infrastructure, Integrated VASCO server, Ericom Terminal Services, Client Side Certificates

Table 1 - Comparison of Benefits

## About AEP

AEP Networks provides a broad range of trusted security solutions, securing data and communications regardless of device, environment or location. AEP's approved security architectures are installed in more than 5,000 organizations all over the world including governments, enterprises and carriers.




**United States**
Toll-Free: +1-877-638-4552
Tel: +1-732-652-5200
Email: sales@aepnetworks.com

**Europe**
Tel: +44 1344 637 300
Web: www.aepnetworks.com

**Greater China**
Tel: +8621 5116 7120

**SE Asia, Singapore**
Tel: +852 2961 4566

**Japan**
Tel: +81 3 5979 2149

**Australia/New Zealand**
Tel: +61 2 9413 2282

**Malaysia**
Tel: +60 32166 2260