aep NETWORKS

Trusted Security Everywhere

Securing the Hybrid Cloud

AEP **White Paper**

for CloudProtect Anytime

CloudProtec
Securing the Hybrid Cloud
Whitepaper

Executive Summary

It's impossible to ignore cloud computing. It's in the press most days and is even advertised on TV; many large IT vendors now offer cloud solutions and organisations large and small are publicising the benefits from their move to cloud computing.

But in reality, moving to the cloud is a little more complex. For most organisations, it means a 2-5 year cloud migration programme, starting with applications that are best suited to the cloud and only moving new applications across when they are as secure in the cloud as they were in the datacentre beforehand.

Throughout the migration period, organisations will be operating a Hybrid Cloud solution, with some of their applications and data in public clouds, some in private clouds probably operated by Hosting Providers and the rest still in their own datacentre. For both IT operations and security this is a difficult phase which must be managed carefully through every change. Of particular concern are the interfaces where the organisation meets the cloud:

- Security tokens need to be exchanged and accounted for
- Data must be transferred securely between the individual, the organisation and their cloud services
- Individuals must identify themselves, ideally seamlessly, to each different application and each data store

AEP's CloudProtect solution addresses a key area of security for the hybrid cloud, providing secure access to applications and data wherever they may be. Today's users don't care where the data resides, but they demand access everywhere from airport kiosks to internet cafes, using a range of devices from smart phones to laptops. Yet the organisation needs to know exactly who is accessing what from where and equally imperative, when people do access that sensitive data, what can they do with it? CloudProtect provides a comprehensive hybrid cloud solution. As a secure remote access solution it is a market leader, supporting the broadest range of secure application access with adaptable levels of user security and comprehensive reporting. As a virtual appliance, it can be deployed by the organisation or their hosting service provider, with all the flexibility and scalability associated with a cloud service.

- CloudProtect Remote is provided on a pay-as-you-use basis to match the managed service providers' business model
- CloudProtect Anytime is a packaged solution for the enterprise that supports a virtual appliance deployment to be operated and managed by the organisation or their hosting service provider on a monthly registered user basis.

In either case, CloudProtect can be supported by AEP's Series E network encryption to establish a secure network tunnel between the enterprise datacentre and the CloudProtect service, minimising the chance of data leakage across the primary enterprise-cloud interface.

Cloud Computing

Cloud computing provides processing and storage on demand to organisations, enabling them to scale their IT at the click of a mouse. IT becomes a service, always available, yet only costing money when it is used. There are many advantages:

- Cloud computing is delivered as a service, paid for as it is used. For large and small users alike, the capital burden of a large IT infrastructure and the risks of under or over provisioning are removed.

- For large organisations, the new flexibility is paramount. Previously they had to invest in large data centres that may only be fully utilised once or twice a year. Now they can turn that processing on and off as they need it.

- SMBs can access a broad range of high quality IT services that were once the sole domain of the large organisation, such as managed email, CRM, document production and accounting.

- All organisations benefit from high availability. A good cloud service provider has many data centres world-wide and can quickly switch processing in the event of a problem. No longer does the IT department have to invest in costly back-up sites or worry about the risk of costly hardware failures.

So why isn't everybody doing it?

In reality, most organisations cannot make just one big switch. Instead, they must look at which applications would benefit most from a cloud based solution and plan their transition to the cloud over time. Most experienced cloud practitioners advise a 2-5 year change programme, with a carefully considered migration of target applications and infrastructure.

The Hybrid Cloud

Throughout the period of migration the enterprise will be using a “Hybrid Cloud”. At any one time, its cloud solution might look like Figure 1, with the organisation delivering its data and applications through a combination of its own datacentre, public and private (hosted) cloud services, for example using:

1. The public cloud (eg Google Docs) for non-sensitive document and media management.

2. The private cloud for email and CRM, from a Managed Service Provider (MSP) or dedicated Hosting Service Provider.

3. Its own physical data centre for sensitive financial, personnel and technical systems.

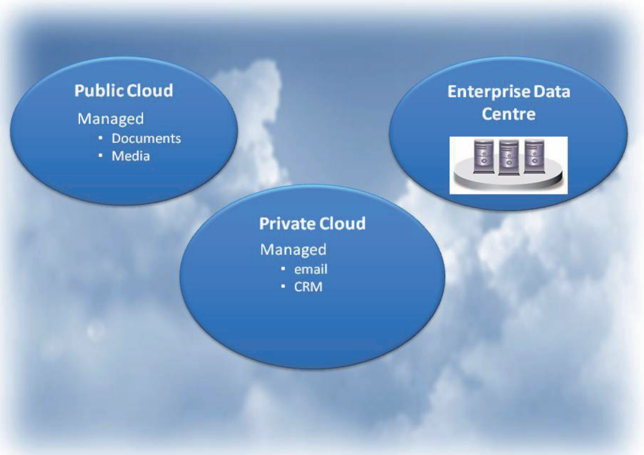

Figure 1 - Typical Hybrid Cloud

Key considerations at each new stage of migration to the cloud are:

- Risk analysis. What risks affect the organisation’s data and assets once they are “in the cloud” and how likely are they to occur. In particular, what new risks are being introduced and what existing risks are being mitigated.

- Cost/benefit analysis. While a move to cloud computing seems to be obvious, there may be hidden organisation and service costs arising from the change

- Service availability. Continuity of service during and after the change is essential. While the cloud seems to offer better availability, is that really the case? Are new single points of failure introduced, such as site to cloud communications?

- Security. When transitioning to the cloud, security remains the responsibility of the organisation. It may be part of the cloud provider’s offering, but it is up to the organisation to confirm that security is adequate for their applications.

Cloud Security

Let us assume that the organisation has completed its risk analysis and is satisfied that the new managed services meet its requirements. It must now model its new IT structure and assess the new security controls to ensure they meet its needs. Here are some of the issues to be considered:

- How secure is my data at rest in the cloud? A simple question, but one which requires in depth analysis of the cloud provider's operation, security measures and controls. Issues range from the quality of data separation inside the cloud to the level of identity checks on external access.
- What protection is there against data leakage? Another simple question with a complex answer. Data leakage can occur both inside and outside the cloud, particularly if gaps arise such that unauthorised people can gain access.
- How secure are the applications running in the cloud? It is essential that the applications themselves cannot be changed without full authorisation, to ensure they cannot be subverted for malicious purposes.
- How good is the audit and compliance support? Even if the security controls are adequate, it is essential that there is a comprehensive activity record to support any later investigation or analysis.
- Some of the security will be provided by the cloud service provider and while security inside the cloud is still evolving, it is becoming much better understood. Internal cloud controls are beyond the scope of this paper, but include:
    - Governance controls, such as compliance, data protection, data discovery, lifecycle management and audit
    - Operational controls, such as business continuity, patch management, application security, key management, identity management and the controls over the virtual environment itself
- Generally, the security of the public cloud must be taken at face value. There is probably little scope for a medium sized organisation to make any changes as the security is designed to match the overall service provided by the public cloud provider. But the organisation can influence private cloud security and any weaknesses can usually be addressed by working with their MSP or hosting service provider to achieve an acceptable solution.

Hybrid Cloud Security

When the hybrid cloud solution is considered as a whole there will inevitably be gaps, especially where the private cloud meets the organisation's people and data in the areas of application security and identity management. Above all, great care needs to be applied where people are accessing applications and data from outside the organisation.

The interface between the private cloud and the enterprise data centre is also important. A lot of sensitive data travels between the enterprise and their MSP or hosting provider and adding network encryption can significantly improve the security of the data in transit.

Secure Application Access

Having successfully secured the Hybrid Cloud solution, let us now consider how the corporation grants legitimate users access to their applications and data. Today's organisation wants its own staff to access their systems from anywhere, and in a variety of ways, perhaps using a smart phone to access email, or a laptop get straight into sensitive data files deep within the organisation.

Secure application access provides a means for users to reach virtually any business resource from anywhere at any time, with a level of access appropriate to the security of the connection.

Traditionally, secure application access has been implemented by an appliance at the edge of the datacentre which controls who does what from where. Ideally in the move to a service model the organisation, or indeed their hosting service provider, can offer users the same service in the cloud, policing access to all applications and data from the cloud rather than from a physical appliance. In that way they can avail of a scalable and disaster proof service, across geographically distant areas, deploying as many virtual machines as needed, with detailed user activity reporting fully aligned to their virtual operation.

What to look for

Good secure 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 Management - A single, common and simple way to manage users and provide controlled access to varied applications, significantly reducing management and operational costs.

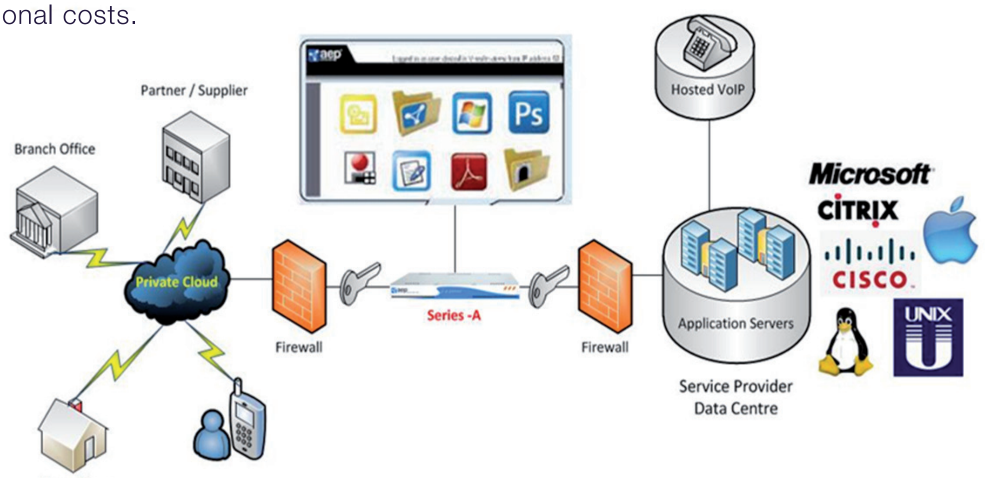

Figure 2 - Secure Application Access

AEP Series A

As a trusted security vendor, AEP delivers a proven secure application access solution. AEP Series A is widely deployed around the globe, 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.

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.

Service providers usually implement cloud security services by adding hardware appliances at their own datacentre, much as in a traditional deployment. Where the cloud service 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 a virtual equivalent of their hardware appliances, their deployment model is still based very firmly on that of the traditional physical appliance.

AEP was one of the first to implement a virtual secure application access appliance and has already gained extensive experience of 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, Microsoft HyperV and Citrix XenServer, providing a comprehensive virtual solution. Multiple instances can be installed as separately addressable appliances, or clustered with a Series A Virtual Load Balancer for unrivalled scale and redundancy.

CloudProtect

CloudProtect is a solution specifically designed to provide secure application access as a cloud based service, enabling rapid deployment to match the flexible, elastic nature of the cloud. It allows customers to deliver Security as a Service (SECaaS) offering a highly secure, policy-based application and network access service that is fully aligned with their other cloud services.

Technically CloudProtect is full feature version of AEP Series A VE running in the private cloud. Comprehensive user reports identify actual usage and there are no hidden licensing or maintenance costs.

CloudProtect is:

- **Highly Secure.** Delivers application, network, and client level security in one solution.
- 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 usage 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. MSPs can embed it as the remote access component of their current cloud offering; enterprises can tailor it and import reports into their existing control panel.
- **Green.** No dedicated hardware. Saves 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.

Figure 3 shows a typical deployment scenario. CloudProtect is deployed as a security service inside the private cloud, which might also be providing email and CRM. It carries out all the user checks (2 factor user authentication, device fingerprint and validity) and applies the correct network security. It then grants the appropriate application access rights to services within the hybrid cloud. This can include mediated access to public cloud services, in addition to access to private cloud and enterprise applications.

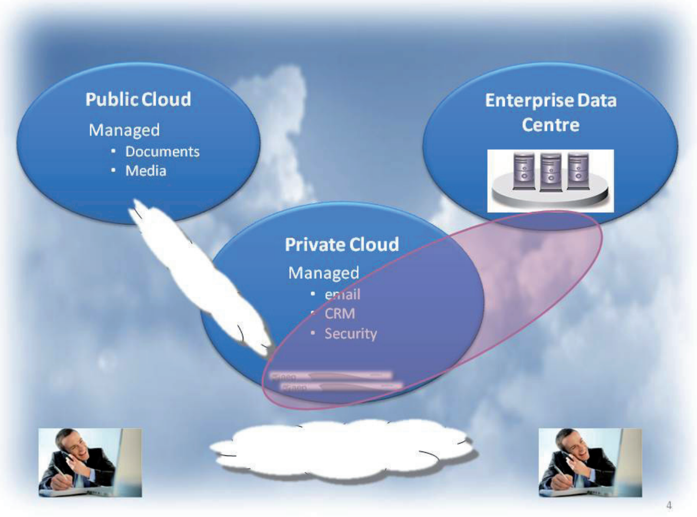

Figure 3 - Typical CloudProtect deployment

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 open-source desktops.

With stringent endpoint policies, CloudProtect removes the danger of an unauthorised device connecting to the cloud environment. Customers can be assured of the integrity of their sensitive data in the private Cloud, as CloudProtect can check every device looking to access applications for full compliance with security standards.

As an option, the link from the private cloud to the enterprise datacentre may be encrypted at the network level using AEP's Series E. This is particularly appropriate if the MSP or hosting service provider is managing the CloudProtect service for the customer, granting authenticated users access to highly sensitive material stored within the enterprise. Without it, the customer would need to secure each application in its datacentre individually, according to need. Figure 4 shows the addition of Series E to the Hybrid Cloud model.

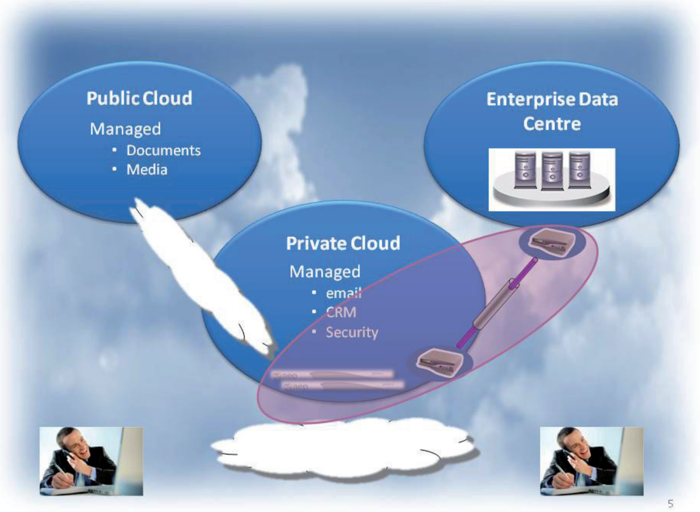

Figure 4 - Hybrid Cloud security with network encryption

CloudProtect Remote for MSPs

AEP's CloudProtect Remote brings industry leading Secure Application Access to MSPs on a pricing model that directly matches the way they sell SECaaS: they only pay for the application security they use, rather than purchasing traditional hardware and blocks of user licenses in advance. MSPs can now scale secure application access on demand, paying only when their customers request it and start using the service. They can offer new services immediately, such as secure remote access to key applications without any significant up-front cost or risk.

CloudProtect Anytime

Many enterprises moving to the cloud prefer to keep control of their own security. CloudProtect Anytime enables them to do so with all the benefits of a true cloud based solution. CloudProtect Anytime is also charged on a usage model, with an all-inclusive monthly licence based simply on the number of registered users for that month. There are no hidden costs for feature licences or additional virtual appliances: the enterprise simply defines their service needs up-front in terms of users and access requirements and selects the most appropriate leasing model. CloudProtect Anytime is also available to hosting service providers, so that they can offer a secure application access service to the enterprise alongside their other hosting services without high up-front risk or investment.

Choosing the Right Solution

For most enterprises, the best solution will be one that fits where they are in the hybrid cloud model. For those just starting out, an enterprise managed solution may be best, as it allows them to keep control of a key security system while they add new cloud services. Later on, a managed solution from their hosting provider may be more suitable or perhaps a move to a fully managed service from their MSP. 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