

## *“Trusted Security Everywhere”*

*AEP Networks provides trusted security everywhere and secures data and voice communication regardless of device, environment or location. Delivering proven security architectures to more than 5,000 organisations all over the world including governments, enterprises and carriers.*

### Products

AEP Networks offers world leading technology that allows IT departments to connect their end users to their corporate applications as securely and reliably as possible. These solutions are designed to not only provide high levels of security but are the fastest to implement and offer the most flexible licencing options for cloud-based infrastructures.

#### LANProtect LanProtect™

*“A secure application access gateway to control application access from any client platform.”*

Users that connect to their corporate applications using Virtual Desktop Infrastructures (VDI) such as Citrix, VMWare or Microsoft Terminal Services are increasingly requesting to connect using a wide variety of devices such as their home PCs, public PCs in airports and even tablets. While these devices can significantly increase overall user productivity, they present a significant security and compliance risk for organisations. LANProtect™ allows organisations to deploy a proven solution to this ever-increasing challenge which ensures that the infrastructure is kept secure while giving end-users the flexibility they demand and reducing the IT department's need to manage individual desktop images. Unlike other licencing schemes, AEP's simple licencing model for LANProtect™ is based on a cost-effective per-user model which does not involve additional license purchases for users wanting to access different VDI components.

#### CloudProtect CloudProtect™

*“A virtualised secure application access gate subscription service to control application access in cloud-based environments.”*

Traditionally, cloud service providers have had to protect their infrastructures and their customers' data in the same way as any enterprise would by paying upfront for security hardware and software licenses. This does not match their subscription-based business models where they are getting paid by customers on a monthly basis. AEP has developed the most innovative security licencing scheme for cloud service providers which does not require any upfront CAPEX spending. CloudProtect™ is a subscription-based, virtualised service that provides Security as a Service (SECaaS) to deliver highly secure, policy-based application and network access.

### Fast facts

- Government, military and enterprise organisations have trusted AEP Networks to develop security technologies for more than 20 years
- AEP has deployed thousands of instances of its next generation Secure Application Access Gateway. This product provides policy based seamless access to applications and secures client end points.
- On June 16, 2010, AEP's Key Security and Management product signed the DNS root of the internet, the dot, forming part of an elite international circle of trust protecting the web from being hijacked
- In Sept 2010 AEP was first to market with Security as a service (SECaaS) for service providers to provide a Secure Cloud Computing environment with utility pricing
- AEP delivers secure deployable narrow band communications to the military and satellite service providers enabling worldwide integrated voice and data communications over slow speed links.
- Partnerships with BT, Fujitsu, HP, Microsoft, Verizon, Cable & Wireless and the UK Government

## ServiceProtect ServiceProtect™

*“A secure application access platform uniquely licensed to match the requirements of public-facing cloud providers who experience unknown high demands on their infrastructures due to their business models.”*

Using traditional security hardware and software licencing models, it is practically impossible for organisations that experience utilisation peaks of their cloud-based services due to the unique nature of their business requirements to size their licence requirements based on the number of anticipated simultaneous users. Getting this sizing exercise wrong could result in the under- or over-provisioning of the security gateway which would result in either leaving the application infrastructure vulnerable to attack during peak utilisation periods or in unnecessary expenditure.

AEP's ServiceProtect™ offers the same high degree of security offered by LANProtect™ and CloudProtect™ but has a unique licencing scheme that does not require the exact number of simultaneous users to be specified upfront. ServiceProtect™ is charged on the number of processors running the Secure Application Access gateway software. This means that service providers with public-facing infrastructures can ensure that they have enough spare capacity to adequately deal with anticipated utilisation spikes without having to go through an expensive, time-consuming and risky license sizing exercise.

## Assurance

*“An additional layer of security to protect confidential data accessed via AEP's CloudProtect™, LANProtect™ and ServiceProtect™ Secure Application Access gateway solutions.”*

LANProtect™, CloudProtect™ and ServiceProtect™ deliver a high degree of security to organisations requiring user access to their corporate applications. However, in order to provide the maximum level of protection for confidential data, an addition layer of security around the cryptographic keys should be deployed. AEP's Assurance integrates with LANProtect™, CloudProtect™ and ServiceProtect™ to deliver an advanced key storage solution that can be used to generate, secure and manage high quality cryptographic keys. The platform is tamper-reactive and is not vulnerable to attack from the network. This all provides the highest level of key security which results in the highest degree of application access security.

## Enhanced Grade Network Encryption

*“IPSec VPN Encryptor that protects IP traffic across open networks.”*

Organisations are relying more and more on the internet to conduct their business and therefore need to ensure that steps are in place to protect the confidentiality and integrity

of their data. AEP's Enhanced Grade Network Encryption allows the deployment of government grade IPSEC based security that protects confidential communications over public and private networks. It also includes advanced central management which significantly reduces the time required for initial setup and on-going tasks such as key change and roll over.

## Key Security and Management

*“A highly secure cryptographic key system that generates and stores high-quality keys in a tamper-reactive device”*

The quality and safe storage of cryptographic keys is critical to the integrity of any key-based security system. AEP's Key Security and Management solution is a Hardware Security Module (HSM) designed to generate excellent quality cryptographic keys due to the quality of the random seed used to generate them. Once generated, the keys are stored in a purpose-built HSM that, unlike others, is not exposed general-purpose operating systems vulnerabilities and positively erases all keys if the hardware is tampered with.

The Key Security and Management system allows the deployment of a high-grade public key infrastructure (PKI) that is both secure and tamper-reactive, positively destroying key material if the device is compromised.

## Secure Communications Optimised Packet Engine

*“Secure traffic optimisation platform for multi-bearer networks”*

Organisations that rely on a variety of bearer technologies to provide voice and data communication between remote and central sites deploy AEP's Secure Communications Optimised Packet Engine (SCOPE) to assist with legacy links that do not interface easily with modern IP networks and low bandwidth links such as 3G or satellite. SCOPE secures and optimises communication in these sub-optimal conditions to ensure reliable and secure data, voice and video communication.

SCOPE platforms are available in network platform, deployable and portable versions which allow groups of users or individuals to benefit fully from the security and optimisation technology.

## Services and Support

AEP Networks have a wide range of professional services, support and training packages available to help install, configure and maintain a secure application access infrastructure. These tiered services are designed to match your business requirements and can provide you with different levels of telephone support and replacement services depending on the criticality of your deployment.

### United States

Toll-Free: +1-877-638-4552  
Tel: +1-732-652-5200

Email: [sales@aepnetworks.com](mailto:sales@aepnetworks.com) Web: [www.aepnetworks.com](http://www.aepnetworks.com)

### Europe

Tel: +44 1344 637 300

### Greater China

Tel: +8621 5116 7120

### SE Asia, Singapore

Tel: +852 2961 4566

### Australia/New Zealand

Tel: +61 2 9413 2282

### Japan

Tel: +81 3 5979 2149

### Malaysia

Tel: +60 32166 2260