

## Case Study: Odeon UCI Chooses AEP Networks' Netilla Security Platform for Secure, Remote Access

Odeon UCI in the UK owns and operates more than 100 multiplex cinemas with 1,057 screens across Europe, the Far East, Asia and South America. With Odeon's senior management traveling frequently between locations it became necessary to provide executives with secure, remote access to email and applications from any location at any time. To make this happen, Odeon installed the Netilla Security Platform (NSP), a Secure Sockets Layer (SSL) VPN solution from AEP Networks, with support and consultancy from Think Secure.

### The Solution: AEP Netilla Security Platform

Odeon chose the AEP Netilla Security Platform over competing SSL VPN vendors because it met all the company's criteria for remote access: advanced security, easy management and flexible user scenarios.

"The NSP ticked all the right boxes at the right price," said Danny Larah, Group Infrastructure Manager at Odeon UCI. "During our selection process it shone above all of its competitors. The first company couldn't even get their system to work; the second was very cumbersome and difficult to use."

According to Larah, employees like the NSP because it offers the same "look and feel" as an office-based PC working environment and provides access to all the applications they need to do their jobs. IT staff like it because they don't need to manage client installations and maintenance on laptops and home PCs. "It requires zero client installation and a minimal amount of IT support, working quietly in the background and leaving us all to concentrate on our everyday jobs," said Larah.

*"AEP has revolutionized our working lives. Workers now access their email, financial reporting systems and other applications in a secure environment."*

*Danny Larah – Group Infrastructure Manager at Odeon UCI*

As part of the total solution provided by AEP Networks and Think Secure, remote users also received key-fob authentication devices that enhance security by providing two-factor authentication. The key-fobs ensure that remote users accessing the company's internal network are, in fact, who they claim to be. Employees can now access their email, the company's financial reporting systems and other applications via the NSP in a secure environment with additional protection.

### The Result

The NSP gives Odeon UCI the power to make mission-critical applications and resources instantly available to employees and trusted partners via standard web browsers while protecting internal networks.

The NSP uses a variety of high-security safeguards including client integrity, an integrated firewall, fine-grained access controls and application layer proxy protection.

For Larah and his team, the NSP has introduced more benefits than they first anticipated. "AEP has revolutionized our working lives," said Larah. "My team and I have our lives back again. If something goes wrong with the network we can sort it out remotely just by logging on to the Internet, with the knowledge that the access is secure."

For example, network errors are fixed faster than ever before because third parties can securely access the network via the NSP. If an engineer needs to fix the network he can do it remotely within minutes simply by logging on to the secure website. As a result, engineer visits have become a thing of the past, as have their expensive fees and travel costs.



Additionally, employees no longer need to carry laptops with them when they travel. They can access applications from any Internet connection, including airport kiosks and Internet cafés. When more executives travel laptop-free it minimizes the risk of losing laptops and information in-transit.

Although Odeon initially offered remote access to senior management, it's now filtering throughout the organization. In fact, there is "never a moment in the day or night" when employees are not logged onto the system.

"At Odeon our SSL VPN solution has proved to be an essential everyday tool which more and more users are enjoying. We now have almost 100 staff using remote access and it's definitely an appliance we wouldn't be without."

### About AEP Networks

AEP Networks ([www.aepnetworks.com](http://www.aepnetworks.com)), the specialist in network and application access security, delivers infrastructure security solutions that are easy to use and manage while offering exceptional value and mission-critical reliability. The company provides a full range of solutions, including identity-based application security gateways, highly secure VPNs, SSL VPNs and cryptographic key management products, to meet the most demanding requirements of public-sector and commercial customers around the world. A privately held company backed by leading technology investors, AEP Networks is based in Somerset, NJ, with European headquarters in London and a Government Solutions Group in Rockville, MD.

### Contact AEP Networks

[info@aepnetworks.com](mailto:info@aepnetworks.com)

[www.aepnetworks.com](http://www.aepnetworks.com)

U.S: 877-652-5200 x5207 • EMEA: +44 (0) 1442 458 640 • Japan: +81-3-3432-3336 • China: +86-571-8702-2892