



SecureWave Partners with Distributed Management Systems to Bolster Secure Remote Access with Proven Whitelist Technology

Milton Keynes, 4 June 2007— SecureWave SA, a worldwide leader in endpoint security solutions, has announced a technology partnership with Distributed Management Systems (DMS). Under the terms of the agreement, SecureWave's Sanctuary® application and device whitelisting software can be incorporated into the DMS CASQUE security system, enabling authorised users to remotely access corporate networks using approved devices and applications.

DMS CASQUE (www.casque.co.uk) provides organisations in the government and private sectors with a complete methodology for strong authentication with active key update and was specifically developed to enable organisations to ensure private access over the internet and thus enable secure remote working. CASQUE users have their own hand held CASQUE Token that receives challenges optically from any workstation screen. This multiple Challenge – Response process denies replay attack and prevents cloning. The CASQUE system can be administered securely by in-house system administrators that do not need to have specialist security expertise. The system is platform independent and allows simple update and control of access privileges.

SecureWave Sanctuary employs a whitelist approach that prevents any application from running and any device from connecting to a corporate network, unless it has been specifically authorised. Anything not included in the whitelist is blocked. This enforces policy-based control over any software applications, executables or devices and enables central management and auditing of everything that runs on a corporate network.

To remove the risk of client workstations being compromised and to ensure that only authorised applications and devices are able to run and connect to a CASQUE-controlled corporate network, all devices will be managed via a whitelist that is centrally maintained and enforced using Sanctuary. Since CASQUE allows for secure authentication without any device being connected, the browser-enabled authentication client application is simply added to the Sanctuary whitelist.

Using the combined solution, remote machines can be secured to limit access for both application and device use, ensuring that only authorised personnel on safe workstations can gain access. New user permissions and whitelist updates can be obtained after successful CASQUE authentication. From the Sanctuary central management console, system administrators can also check what permissions are installed per client.

“CASQUE was developed with specific intention of enabling corporations to extend their networks to enable remote access over the internet, without risking security breaches,” said Bertrand Manhe, Director of Strategic Alliances of SecureWave. “This perfectly complements the Sanctuary approach which gives IT managers absolute control over what is allowed to run on the network and yet is granular enough to allow authorised employees to access whitelisted applications and use specific devices at permitted times.”

Commenting on the partnership, Basil Philipsz, Managing Director, Distributed Management Systems said: "We want CASQUE to be the option of choice for secure remote access where non-repudiation, ubiquity of client and assurance at an EAL4 level is obtainable at no extra cost. We believe that Sanctuary elegantly solves the "Endpoint" problem as we can confidently verify client health as part of the User Authentication Process."

Sanctuary has DIPCOG and Common Criteria certifications whilst CASQUE has DIPCOG and CESG CAPS certifications.

About SecureWave

With SecureWave's Sanctuary®, organisations set and enforce policies for device and application use that overcome tomorrow's security and operational challenges today. More than 1,700 enterprises worldwide in the financial, government, military, manufacturing and healthcare sectors, including Lockheed Martin, CSC/Anglian Water Services, MTU, Barclays Bank PLC and Norwich Union, utilise Sanctuary. SecureWave, named a Red Herring Top 100 Innovator, is headquartered in Luxembourg and services its global customer base via offices in the U.K. and Herndon, VA, as well as through a network of reseller and service provider partners worldwide. To learn more about SecureWave, please call +44(0)1908 357897, or visit www.securewave.com.

About Distributed Management Systems

Distributed Management Systems is a private, UK owned company with offices in Blackburn, Lancashire, UK. Distributed Management Systems' main Product Line is CASQUE. CASQUE is a patented method and means for providing complete security systems including authentication, key update, key recovery and administration. CASQUE Systems are administered completely in-house by non-security experts and are capable of providing definable risk assessment and supporting the highest levels of assurance. For more information, please contact Margaret Tate marg@casque.co.uk.