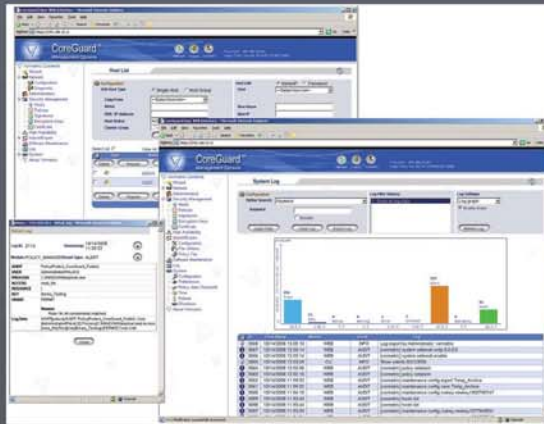


PRODUCT review



## Data Security Server from Vormetric

The number and scale of recent data security breaches can't be down to a lack of security solutions as there are a good range of products on the market that can stop these in their tracks. A prime example is Vormetric's Data Security Server (DSS) which delivers tough data encryption but also combines this with the ability to protect databases, applications and file systems from a wide range of threats.

DSS is deployed as a central appliance and uses PEMs (policy enforcement modules) on the host systems that are to be protected. Separate PEMs are available for file systems and databases and not only do they have a low impact on resources, but the complete solution can be deployed in a matter of days. For testing we used a selection of Windows Server 2003 R2 systems as hosts and found that installation is, indeed, a simple task.

The appliance provides two dual-personality Gigabit data ports for copper and fibre connections and a dedicated port allows management access to be isolated. There's a HA (high availability) port and up to 24 appliances can be linked together for massive redundancy. The appliance is physically tamperproof and if it is opened, its encryption keys will expire immediately. There's also a panic button on the front panel for dire emergencies but in either event all keys are backed up and can be recovered.

CLI, SSH and web browser access is supported and we opted for the latter where we were greeted with a well designed interface that is very easy to use. Each network port can be configured for management or PEM communications and three administrator types are supported where the master has full control. One can change security settings and another can only modify network parameters. PEMs are installed locally on each system to be protected and are then added to the appliance as new hosts.

Once a host IP address has been entered, the appliance detects the new system and automatically and transparently set up encrypted communications with it. Policies define what you want to protect and contain rules that specify users, actions, effects, file types and applications. Users and groups can be added from Active Directory or via LDAP and protected resources range from a folder or database, to a registry entry.

We created protected folders on our hosts and then placed a selection of documents in them after the policy had been applied. We selected users that were allowed to view and open the folders and if an unauthorised user tried to make access, they received an error message. The protected directories could no longer be viewed by Windows Explorer and any attempts to use other applications to access them proved

fruitless. Furthermore, with policy auditing selected, we could see all attempts to access protected folders and which users were involved.

You can also control which applications can access protected data. Once defined, a signature is created from the application executable and you can also include all associated DLLs. When a user attempts to access protected resources, the signature of their application is compared and permission will only be granted if there is a match. HIP (host image protection) takes security a stage further by creating signatures for every file type and application on selected systems - useful for protecting web servers that are fully exposed to the Internet and also for implementing change management controls.

DSS delivers strong data protection measures and we were impressed with how easy it was to deploy. It offers regulatory compliant auditing and logging, and once it is up and running it is virtually transparent to general business operations; save for its protection. **NC**

**Product: Vormetric Data Security Server 3.4**

**Supplier: Digital Pathways Ltd**

**Tel: 0870 321 4002**

**Web site: www.vormetric.com**