THYCOTIC SECRET SERVER

Privileged account credentials are the number one target for today's cyber criminals, as they provide easy access to the very heart of a business's IT infrastructure. They are the top of the list for compliance and security audits, so businesses must control access to these critical accounts to stay on the right side of data protection laws.

Thycotic's Secret Server is an elegant solution for managing and auditing privileged account access. It uses a hardened vault to store account details, keys and certificates, provides privileged account discovery and augments them with fully automated password rotation enforcement.

This latest version introduces a range of new features, with the distributed engines delivering improved throughput and scalability across global infrastructures.

The new RDP proxy leverages Secret Server's Jump hosting feature, allowing businesses to provision secure access to third parties, such as consultants, without revealing privileged account credentials.

We found deployment in the lab a swift process and used a Windows Server 2012 R2 system to host it. Along with IIS, it requires an existing SQL Server database and we loaded the free SQL Server 2012 Express. Thycotic's documentation covers system requirements and the installation process clearly. Prior to loading Secret Server, we created a new SQL database and administrative user from the Management Studio as instructed and were ready to go inside 30 minutes.

The Secret Server web console is very well designed and we used its widgets to customise it, as required. The Advanced view provides full access to all features, but you can limit this to the Basic view for some users, so they can only access specific managed resources.

Secrets define details of privileged accounts and associate user names and passwords with domains, hosts, machines, web sites and so on. Thycotic provides a good selection of predefined templates, including ones for AD, SQL, Unix, Cisco and SonicWALL network devices, web sites and Windows accounts.

We quickly integrated Secret Server into the lab's AD domain and used its slick discovery tool to import all users with administrative privileges. Account roles could then be assigned to determine permissions, allowing us to strictly control access to specific secrets.

Security is tight, as all secrets are stored in the vault, using AES-256 encryption. The Enterprise edition also offers the DoubleLock feature, which applies an extra encryption key, using a second password.

Secrets are accessed from the home page and each one has a Launcher icon that loads the relevant application. Users can be blocked from seeing the actual password for the resource they're accessing and we recorded sessions using the Xvid video codec on our host. Each secret can also automatically generate new complex passwords, using regulatory compliant formats.

Secret Server discovers local admin accounts on Windows systems, changes their passwords using policies and rotates them regularly. It's also a great tool for securing virtualised environments, as it can discover privileged accounts on VMware ESXi hosts and ensure the root password is changed regularly.

Rules make Secret Server even more versatile, as they can, for example, be used to identify new and unknown privileged accounts and bring them under its control. Staff movements aren't a problem either, as you can see what they accessed from Secret Server's regulatory compliant audit logs. Applying the Expire Now feature to the relevant secrets causes the passwords on every account they accessed to be changed immediately.

Privileged accounts are the crown jewels of a business and must be protected at all costs to avoid potentially disastrous data breaches. Secret Server is an ideal solution, as it can be deployed in minutes and provides a powerful set of tools for regulatory compliant password management. CS

Product: Secret Server
Supplier: Thycotic Software
Tel: +44 (0)203 608 4323
Web site: www.thycotic.com