ESET Tech Center

Encryption with network servers

Anish | ESET Nederland - 2018-02-16 - Comments (0) - ESET Endpoint Encryption

Encryption of data stored on a network file server is possible. However due to its effect on the user base and the variety of host environments the process should be fully understood before deploying to a live server.

Using encryption with a server does not provide any audit report of access other than those already provided by the host operating system.

There are two methods of encryption that might provide the required security.

Granular encryption

It is possible to run DESlock+ on the connected client machines and use the software to create encrypted containers to store sensitive data on the server. This method can also be used with non-Windows file servers and Network Attached Storage devices. The container types detailed below would be suitable for this purpose:

Encrypted Archives
Individually Encrypted Files
Encrypted Virtual Disks
Text encrypted using text encryption

It is **not** possible to use folder encryption over a network, please see this article for more details: I am unable to encrypt a network folder

Full Disk Encryption

It is important to understand the attack vector being defended against and how Full Disk Encryption functions before considering it as a solution for securing a network server.

For ease of maintenance FDE should only be used in a server environment

where absolutely necessary. Using Full Disk Encryption will prevent files being accessed or copied from the machine only once it is powered off or restarted.

When a system is full disk encrypted, once you have authenticated yourself with your credentials through the DESlock+ boot loader the system will provide files and share data just as it did before encryption.

FDE does not provide any further levels of access control than provided by the operating system itself. It does not prevent data being retrieved from the server across the network by an attacker exploiting the operating system itself.

If this is the attack vector being defended against then using an encrypted container stored on the server such as a virtual disk and accessed by the clients using DESlock+ at the client end would be a more suitable solution. This has the advantage that only the necessary sensitive data is encrypted. However it should be kept in mind that only the first person to mount a virtual disk from the network gets read/write access, subsequent users will get read only access until the drive has been un-mounted by all users.

If Full Disk Encryption is required then the following caveats should be kept in mind when implementing the encryption:

> You should ensure that the encryption process and backup/disaster recovery procedures are tested fully on an identical server setup (both hardware and software) before deploying to a live server.
> It is important to verify the solution works correctly with the same disk controllers and drives being used for storage on a test server. This is especially important if the machine uses RAID storage.
> There will be a performance overhead due to the encryption which should be borne in mind if the server is under high demand.
> If admins use remote desktop connection or similar remote connection software then they need to be aware rebooting the system will require someone physically present at the server machine to login through the DESlock+ bootloader should the system need to restart for any reason, for example when applying OS updates. By installing DESlock+ version 4.8.17 on a Workstation with a Trusted Platform Module (TPM) enabled, it is possible to configure the 'No Extra Authentication' mode. This mode doesn't require authentication at the DESlock+ bootloader so the user will boot straight to the Windows logon. It is important to note that this will then shift security to the Windows logon. Please see the articles below for more information:
>
> KB430 - Trusted Platform Module (TPM) Support
>
> KB439 - Trusted Platform Module (TPM) FAQ

> Note: there are some remote hardware keyboard devices that should in theory allow login through the bootloader as they load with the BIOS of the machine.

If the encrypted machine is to be managed by an Enterprise Server, it is important the Enterprise Server is not hosted on the same machine. This is because access will be needed to the Enterprise Server to recover the FDE logins should the FDE login credentials be forgotten. To give a real world example, it is like locking the emergency code for a safe inside the safe.
It is only possible to Full Disk Encrypt Windows machines. It is not possible to full disk encrypt NAS devices or Linux based servers

---

Keywords: nas fileserver domain encrypt server encryption server network