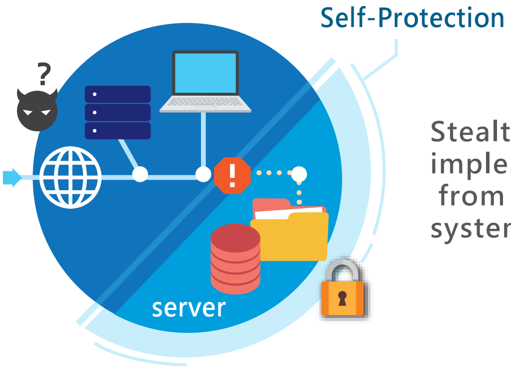
TrustONE Stealth Defense

Advanced Anti-ransomware Solution for DB and Backup Server

The Introduction of Stealth Defense

Stealth Defense employs Stealth Defense Area technology to safeguard critical data on the Production Server, including the Database Server, Exchange Mail Server, File Server, and Backup Server.Stealth Defense employs Virtual Stealth Defense Area Technology to render critical data invisible, thereby deceiving hackers and ransomware. Moreover, the Self-Protection of Stealth Defense can stop the attacks from hackers and ransomware. Therefore, the critical data of production sever can be free from stealing and encryption.



Stealth Defense Area technology can create a secure isolation zone which implemented at the driver layer, . This zone prevents hackers and ransomware from accessing server sites or file folders by exploiting security gaps and system vulnerabilities.

The Self-Protection of Stealth Defense

Kernel Protection：This feature safeguards the operating system's kernel mode. Even if a hacker gains system administrator privileges, Stealth Defense's protection cannot be disabled or altered.

Anti-Erasing：Stealth Defense ensures that isolated and protected files cannot be removed or overwritten by hackers or ransomware.

White List：Only authorized processes have access to files within the Stealth Defense Area.

Applications and software on the White List are allowed to run in the Stealth Defense Area. Conversely, ransomware and malicious codes are prohibited from executing in this secure zone.

The Protection Scope of Stealth Defense

01.
SQL Database

Stealth Defense protects MS SQL data, allowing only MS SQL-related processes access while blocking ransomware.

02.
Exchange Mail Server

Stealth Defense secures Exchange Mail Server data, permitting only Exchange server processes access and preventing ransomware infiltration.

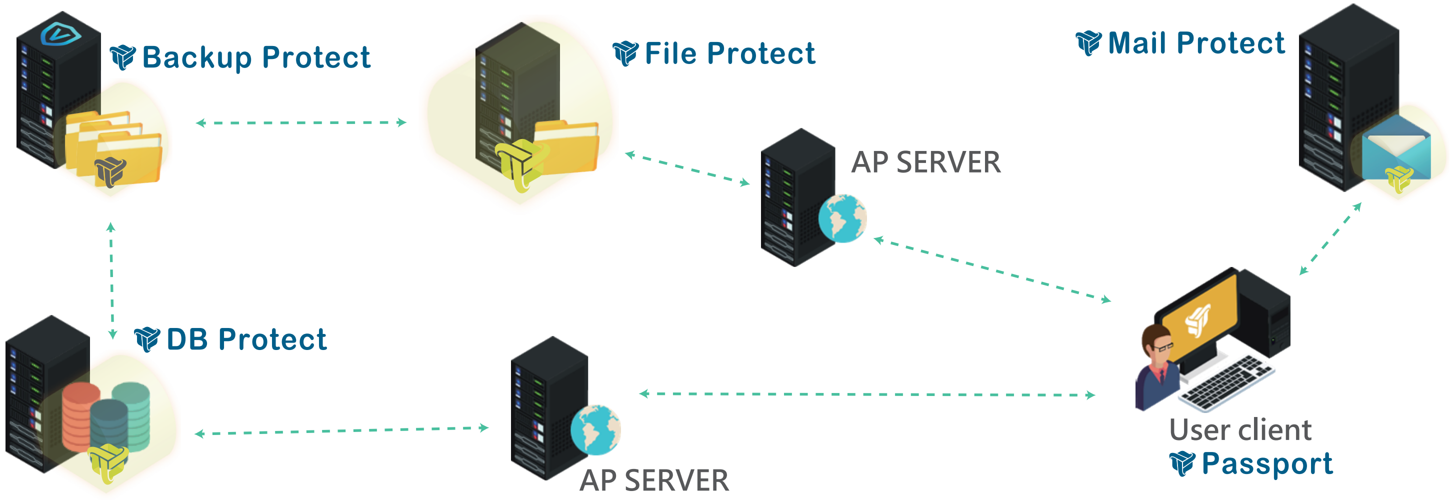
03.
File Server

File Server/NAS documents are shielded by Stealth Defense, enabling access only through user client Passport via the Tunnel Server, with ransomware access denied.

04.
Backup Server

Backup Server data is safeguarded by Stealth Defense, granting access solely to Backup server processes and barring ransomware entry.

Stealth Defense Sysetm Architecture



System Requirements

TrustONE Server/Passport	Recommended PC Spec
TrustONE Server： -Microsoft Windows Server 2012 R2 to 2022 standard or above -Linux Unbuntu 20 / Cent OS 7 / Red Hat 7.9 or above TrustONE Passport： Microsoft Windows 8.1 to 11 Home edition or above	TrustONE Server： -Intel Xeon E-Series process or above -16GB RAM or above 100GB hard disk space or above TrustONE Tunnel： -1 Gbps or above Ethernet network card. TrustONE Passport： -4GB RAM or above is required according to the official requirement of the operating system and application -250MB of free hard disk space