

ARROSOFT STEALTH

D A T A S H E E T

Arrosoft Stealth – You can't hack what you can't see

Insider threats in cybersecurity, originating from employees, contractors, or partners with legitimate access, pose significant risks to businesses. These threats can be malicious or unintentional, leading to financial loss, reputational damage, and operational disruption. Insiders can more easily bypass security measures, resulting in data breaches, intellectual property theft, and fraud. This not only incurs remediation costs and legal consequences but also erodes customer and partner trust. Mitigating these risks involves robust access controls, continuous monitoring, comprehensive security training, and fostering a culture of security awareness.

Arrosoft created Stealth solution as a countermeasure to the insider threat scenario which is becoming more prevalent in this day and age. Arrosoft Stealth, much like a stealth fighter, operates by rendering critical files and servers invisible to potential adversaries. Just as a stealth fighter uses advanced materials and design to evade radar detection, Arrosoft Stealth employs sophisticated methods to obscure the presence of sensitive data and systems from hackers. Additionally, it incorporates robust authentication mechanisms to verify the identity of users and devices before granting access. This dual approach ensures that only authorized entities can interact with the hidden assets, significantly reducing the risk of targeted cyberattacks and enhancing the overall security posture of the organization.

Arrosoft Stealth capabilities



PROTECT YOUR SERVERS

You can't hack what you can't see. Arrosoft Stealth restricts critical systems from unauthorized access on your network.



PROTECT YOUR DATA

Arrosoft Stealth hides critical data files and folders and limits access to only select privileged users.



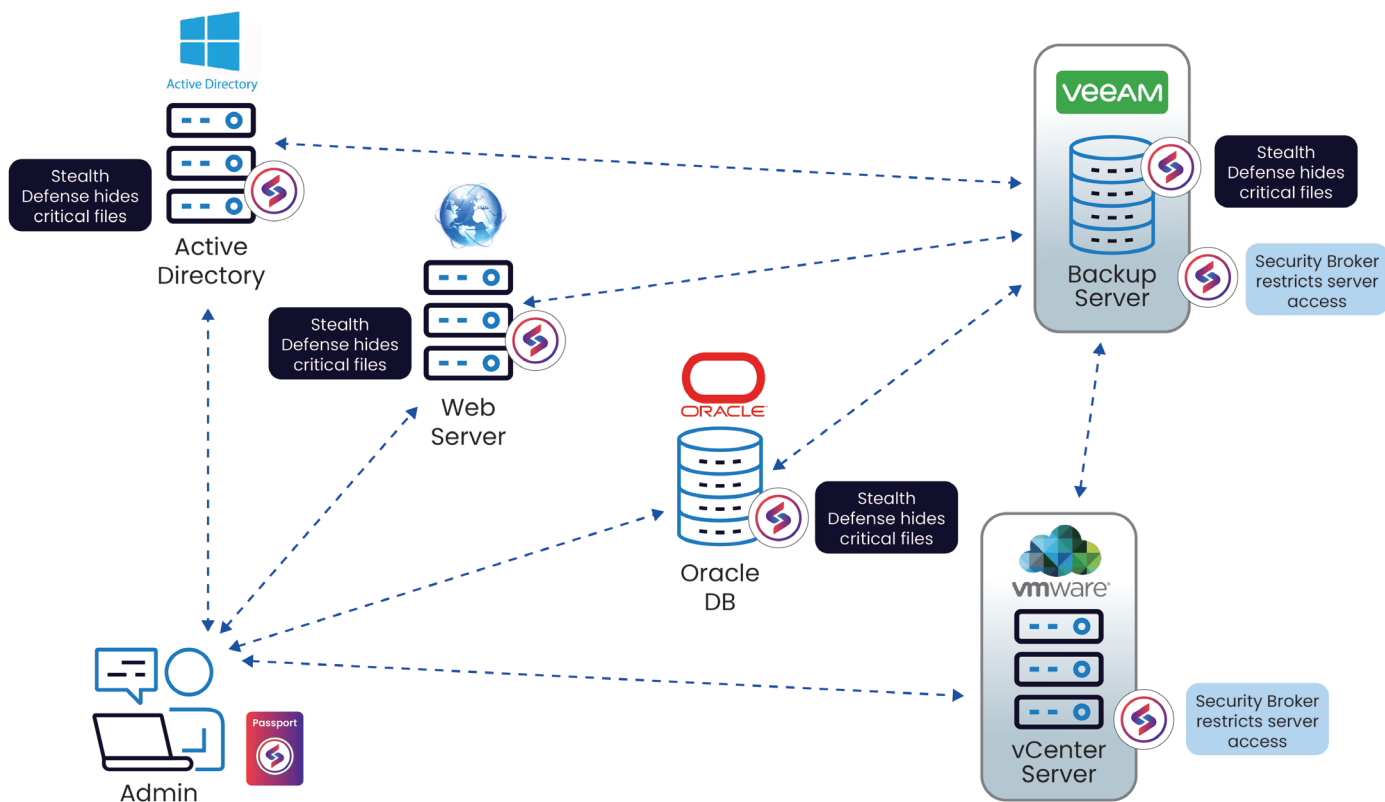
PROTECT YOUR ACCESS

Limit and protect your access to critical systems and data by using active authentication and zero-trust security.

Arrosoft Stealth protects your database, file and application servers and backup servers in a multi-layered approach.

ARROSOFT STEALTH

DATA SHEET



Stealth Defense technology establishes a stealth isolation zone at the driver layer. This zone effectively prevents hackers and ransomware from accessing server sites or file folders by exploiting security gaps and system vulnerabilities. Stealth Defense secures your data by utilizing the following techniques:



KERNEL PROTECTION

This feature secures 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 guarantees that files in isolation and protection cannot be deleted or overwritten by hackers or ransomware.



WHITE LIST

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