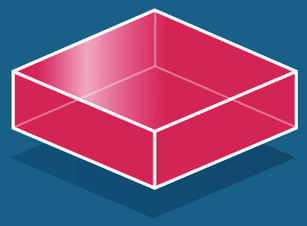


eReD HYPERVISOR SECURITY

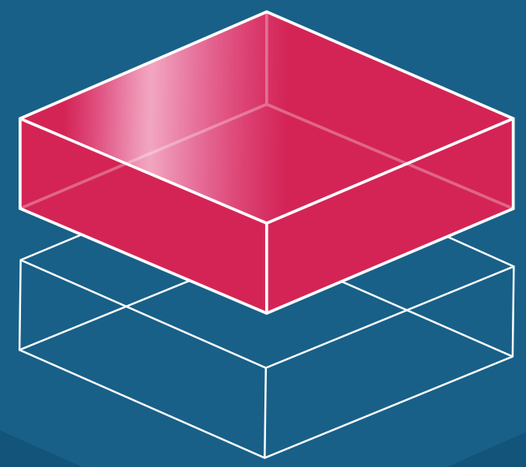
SOOSAN INT

SOOSAN INT Co., Ltd. #3F, Suseo Hyundai Ventureville, 10, Bamgogae-ro 1-gil, Gangnam-gu, Seoul, Korea 06349
+82 (2) 541 0073 | esales@soosan.co.kr | www.soosanint.com

ReD HYPERVISOR SECURITY

Next Generation Hypervisor Security

Blocks Malware including Ransomware
Protects Important Data
Provides Virtual Machine Security



SOOSAN INT

VS

New attacks are discovered everyday

- New rootkits that can bypass anti-virus and other security solutions
- System penetrating fileless malware
- Unknown/zero-day attacks that can corrupt or exfiltrate system data

eReD Hypervisor Security is hidden protection

- eReD protects even systems that have been rooted
- eReD protects important data from fileless malware by controlling file access
- eReD blocks all types of attack including unknown malware using whitelist-based application control

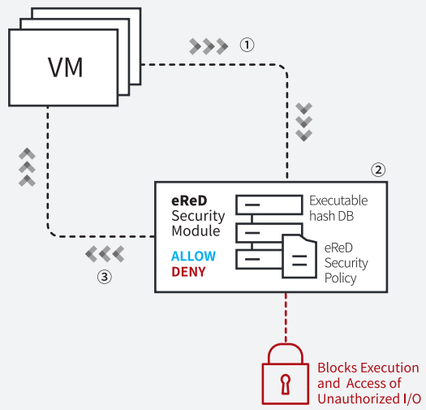
Main Features

Uses VMI
(Virtual Machine Introspection)
for hidden protection

Protects important data against exfiltration/tampering/damage using access control

Using whitelist based application control, completely blocks malware including ransomware

Application/File Access Control Flow



① All file I/O from the VM is transferred to eReD security module in the hypervisor.
② eReD checks the I/O against user created security policies and whitelisted application hashes stored in the DB.
③ Only authorized I/O is allowed to run on the VM.

VMI (Virtual Machine Introspection)

Using Virtual Machine Introspection, or VMI, eReD has visibility into VMs through the hypervisor. eReD can control and monitor file I/O for important data from the VMs, from the hypervisor, a separated layer.

Data Protection using Access Control

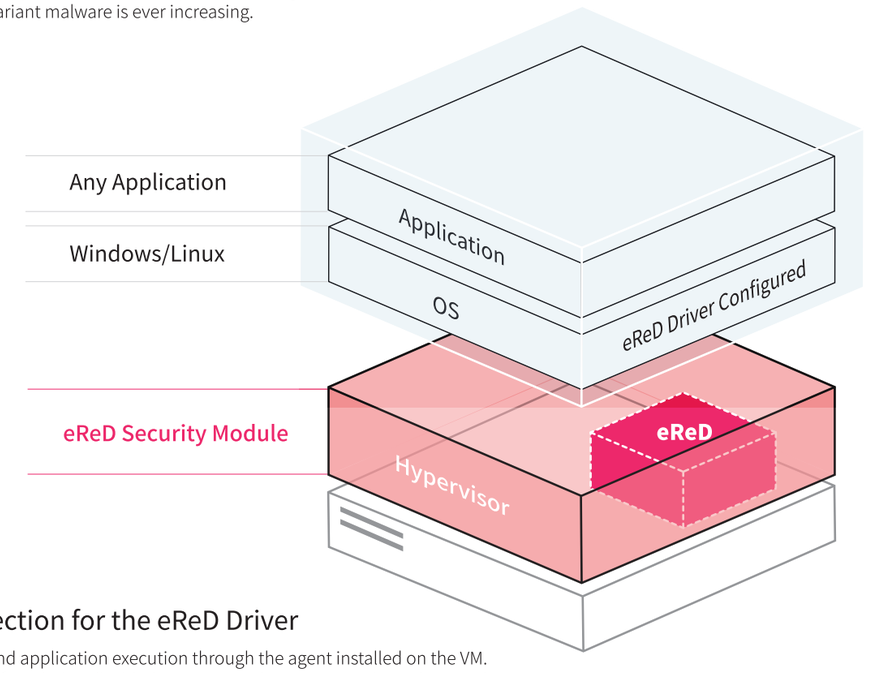
eReD takes an original approach by using VMI to control file access and application execution for the first time in the world. First, the administrator configures files to protect and processes/users to allow access to them. Then eReD protects the configured files against exfiltration, tampering, and damage.

White List based Application Control

eReD controls applications by a whitelist of permitted applications. The hash values of all applications(exe, dll, etc.) from the VMs are calculated and stored outside the VMs in the hypervisor. Every application's hash is checked against the whitelist and non-listed applications, including malware, are blocked.

Blocks All Unknown Malware / Zero-day Attacks

Using the white-List method, eReD blocks all sources of attacks more thoroughly than other malware detection/analysis solutions. eReD provides next-generation security in an age where new and variant malware is ever increasing.



Double Self-Protection for the eReD Driver

eReD controls file access and application execution through the agent installed on the VM.
To prevent the eReD agent from being disabled, eReD not only prevents registry changes, but also protects memory allocated to the eReD agent from outside the VM in the hypervisor.

Separation of the VM and Security Layer

By design, eReD isolates service from security by enforcing security from outside the VM in the hypervisor. eReD monitors I/O from outside the VM, hiding it from attackers, so even if a system is rooted, eReD cannot be disabled or circumvented.

Key Benefits

Security is enforced from outside the VM, preventing attackers from being able to disable it.

Blocks all types of attack including unknown malware

Access control policies protect important data against exfiltration, tampering and damage

Provides log visualization via a web-based dashboard

Integrates eReD log data with your SIEM to enhance your organization's security.