The beginning of a new era, not just a new security solution

eReD HYPERVISOR SECURITY

SOOSAN INT

eReD

Completely blocking unknown attacks

to create a secure virtual server

Problems that must be solved :

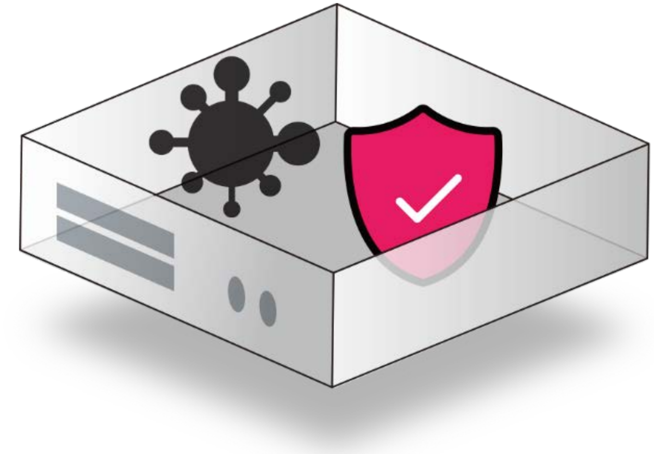
Malware, including ransomware

Security being disabled or bypassed

Unknown vulnerability targeting zero-day attacks

New attacks are always being created.

Anytime they could penetrate, hide and bypass or disable your security solutions.

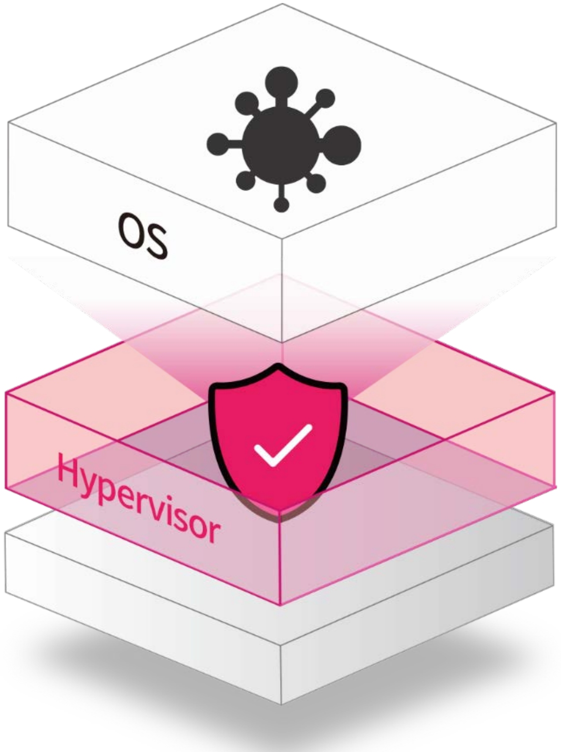


Existing server security solutions

defend against malware from inside the server OS.

The reasons Other solutions fail

- When an attacker roots a system or gains the system admin role, using admin privileges, the attacker can disable security programs.
- Because other solutions run on the OS, it's difficult to detect or block system penetrating attacks by hackers or malware.
- Other solutions often can't detect or respond to new, variant, or zero-day attacks.
- Existing white-list based security solutions run inside the OS, so they can be disabled or bypassed



eReD Hypervisor Security

eReD, a new era starts

"Before any attack can succeed it must first disable or bypass the server's security."

- eReD protects from a separate layer located outside the virtual server.
- Attackers don't have visibility outside the virtual server, making impossible for them to connect to or disable eReD.
- eReD has visibility into all activity on the server, but because attackers can't see eReD, they can't find what to bypass or even how to bypass eReD.

The result is that all attempted attacks will fail

What eReD HYPERVISOR SECURITY Provides for you

01.
Blocks original attacks

02.
Security that cannot be disabled

03.
Support for many Types of servers

04.
User-friendly UI

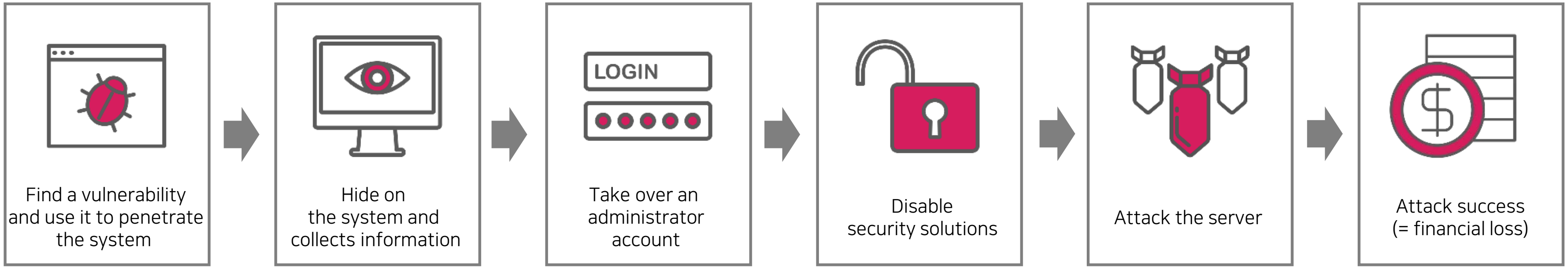
05.
Efficient use of server resources

01

The only thing staying ahead of attackers, eReD.

Blocks original attacks

To take ownership of important server resources, steps like these must be used:



Find a vulnerability and use it to penetrate the system

Hide on the system and collects information

Take over an administrator account

Disable security solutions

Attack the server

Attack success (= financial loss)

With eReD,
attacks will fail from the very first step.

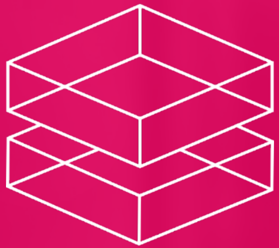
02

The security layer that an attacker cannot reach - like a mirage.

Security that cannot be Disabled

Security layer outside the service layer

- eReD protects servers by separating the security layer and the server (OS) allowing complete monitoring and control of the server.
- eReD cannot be disabled even if an attacker gains administrator rights because the security module is impossible to find from the server VM.



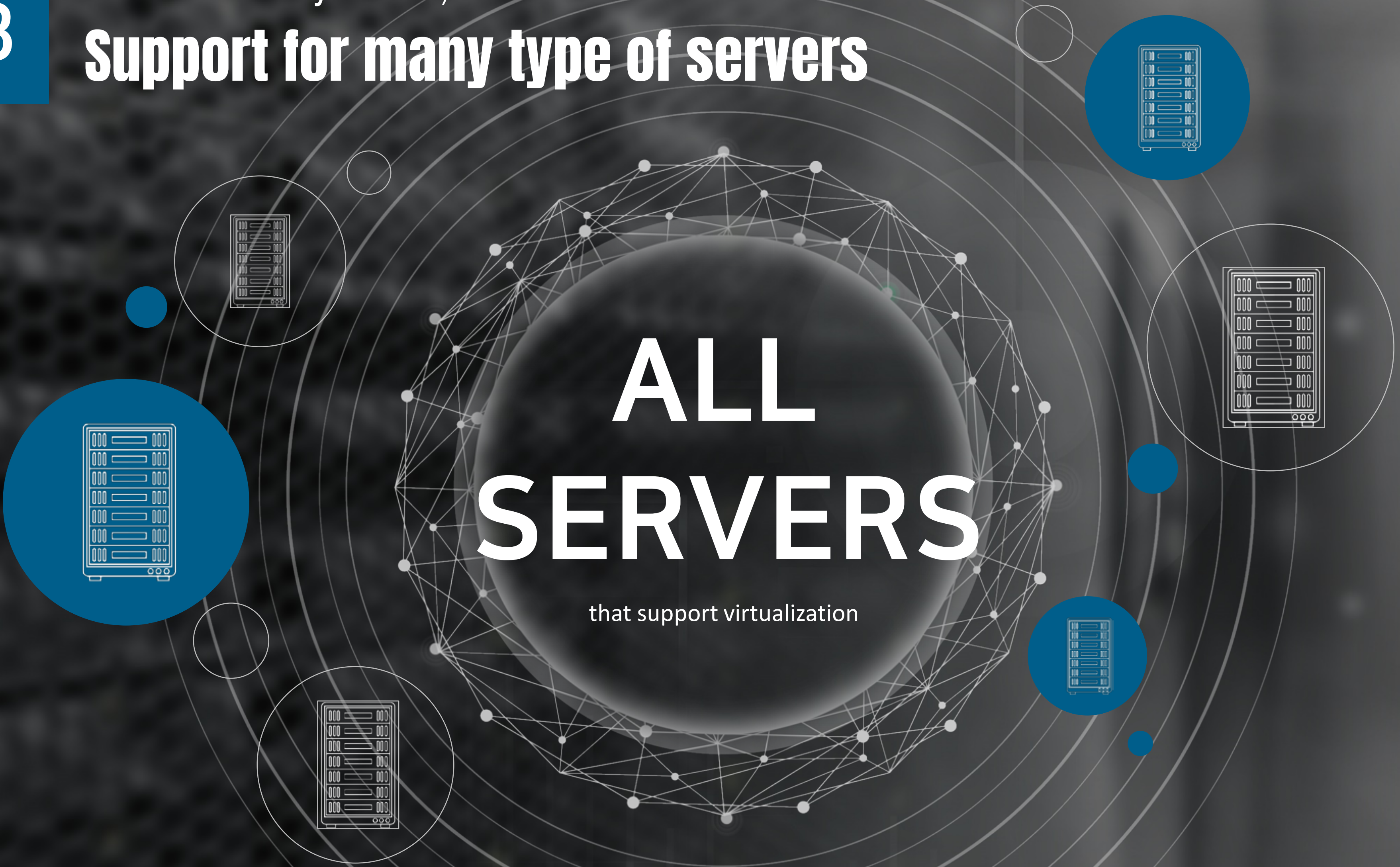
VMI (Virtual Machine Introspection)

VMI is a technology that enables monitoring and inspection inside a virtual environment using the hypervisor.
eReD is the first solution the world over to use VMI for file access control. It’s engineered to monitor and control VM File I/O through a security module located in the hypervisor.

03

Whatever server you need,

Support for many type of servers



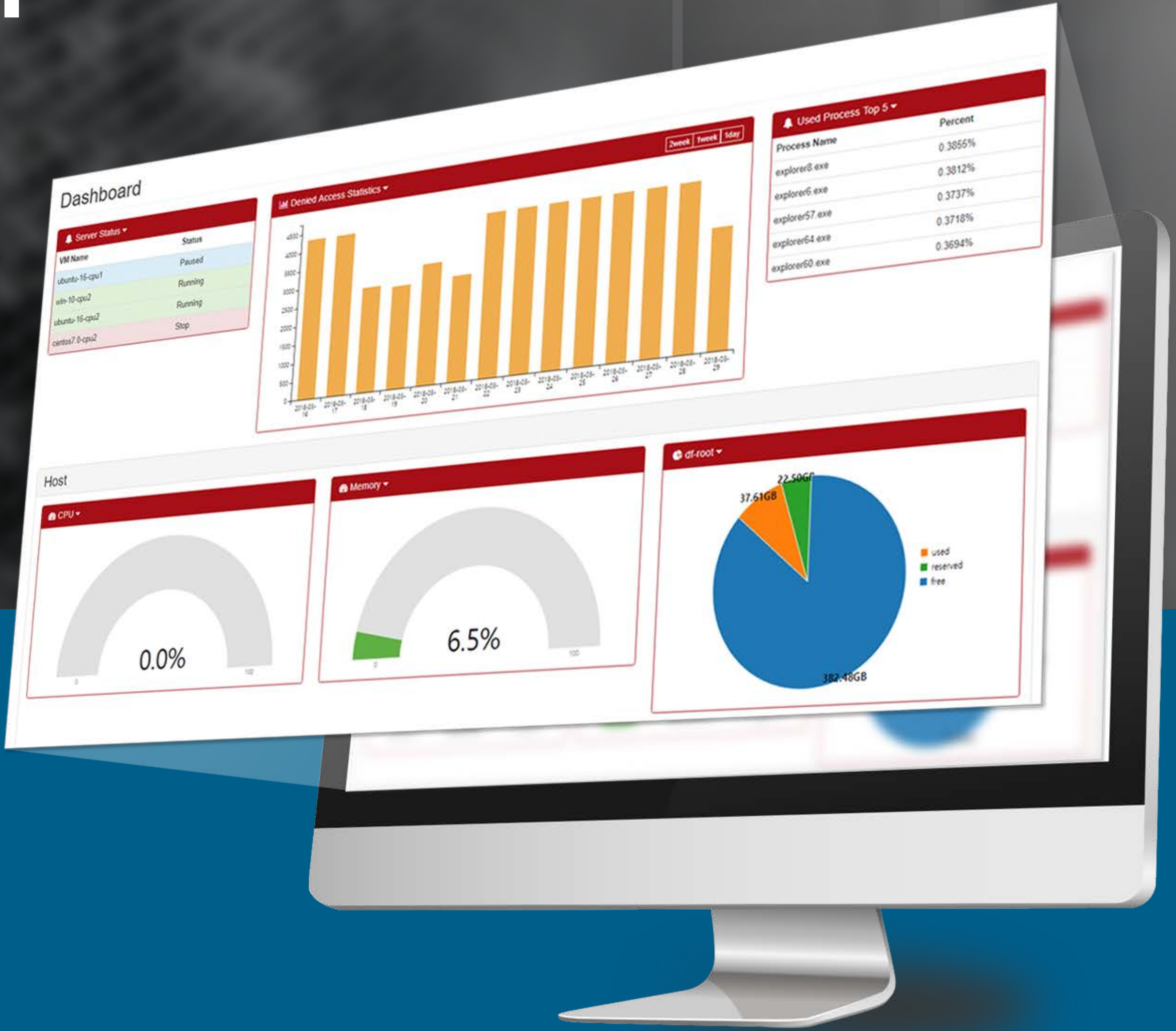
ALL SERVERS

that support virtualization

04

Uniquely convenient, usable at a glance

User-friendly UI



Dashboard

Server Status

VM Name	Status
ubuntu-16-cpu1	Paused
win-10-cpu2	Running
ubuntu-16-cpu2	Running
centos7.0-cpu2	Stop

Used Process Top 5

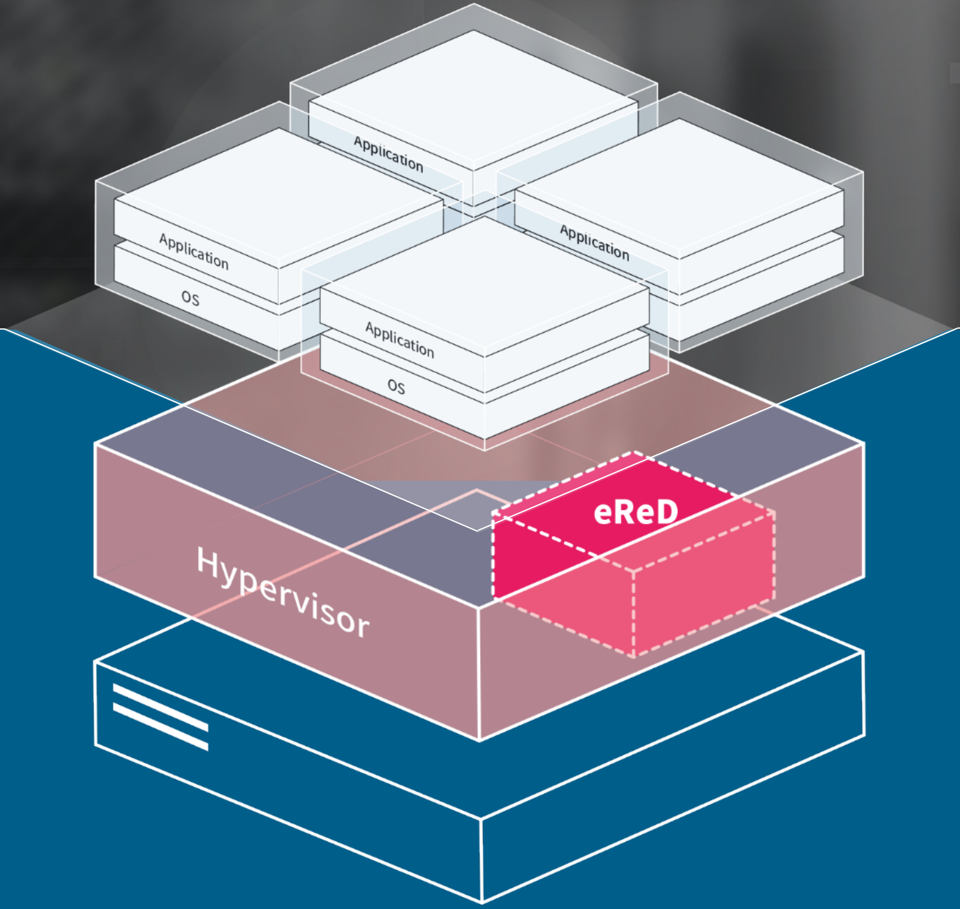
Process Name	Percent
explorer8.exe	0.3855%
explorer6.exe	0.3812%
explorer57.exe	0.3737%
explorer64.exe	0.3718%
explorer60.exe	0.3694%

05

Multiple VMs, one server

Efficient use of Server Resources

- Make more efficient use of idle server resources
- A single server can support several VMs
- Reduce costs by virtualizing your servers



ReD HYPERVISOR SECURITY

Main Features

01.

File access control

02.

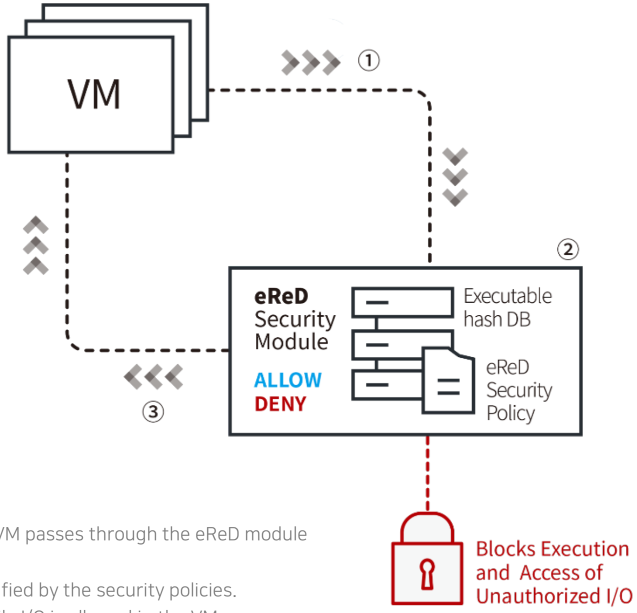
Application control

03.

Logging/ monitoring

01 File access control

eReD provides powerful hypervisor security with file access control.
To protect important data from exfiltration, tampering and damage eReD allows users to set protected files and the processes and users allowed to access them.



1. File I/O from the VM passes through the eReD module in the hypervisor.
2. I/O request is verified by the security policies.
3. Only authorized file I/O is allowed in the VM.

Detailed Policy Controls for Protected Files

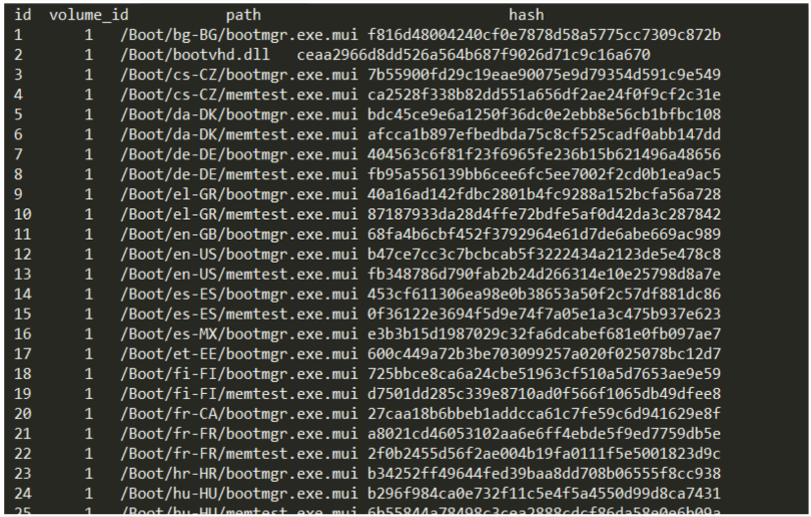
(Ex.1) Allow read only: Protects from tampering and damage.
(Ex.2) Allow execute only: Prevents the protected files or directories from tampering.

Allows Access From Specified Applications Only

Even with a compromised administrator account, the specified files cannot be accessed
(Ex.1) Allow only applications related to the web server to access web source files.
→ Exfiltration and tampering are prevented because it’s impossible to access the web source through other applications.
(Ex.2) Allow only authorized DB programs to access DB files
→ Exfiltration and tampering are prevented because the DB files can’t be accesses by other applications.

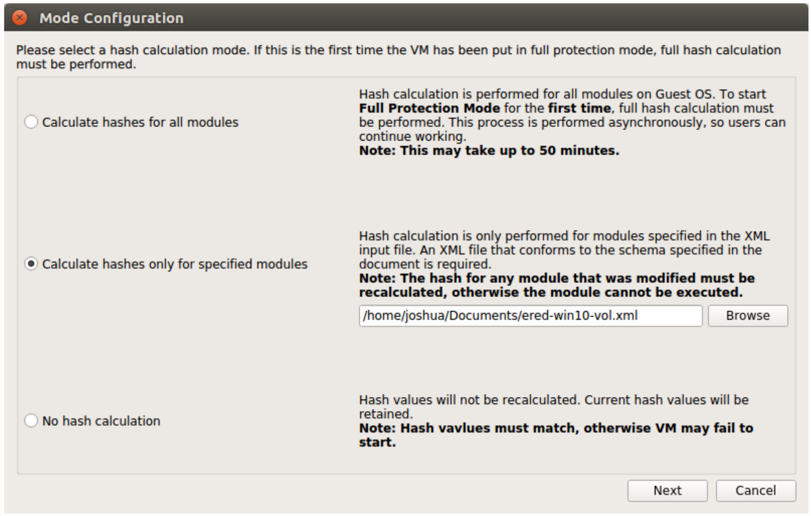
02 Application Control

eReD controls application execution through the use of a whitelist. eReD stores hashes for all executables (exe, dll, etc.) that are on the VM, and completely blocks the execution of all unauthorized applications including malware and executables where tampering has occurred.



```
id  volume_id           path                               hash
1        1   /Boot/bg-BG/bootmgr.exe.mui f816d48004240cf0e7878d58a5775cc7309c872b
2        1   /Boot/bootvhd.dll   ceaa2966d8dd526a564b687f9026d71c9c16a670
3        1   /Boot/cs-CZ/bootmgr.exe.mui 7b55900fd29c19eae90075e9d79354d591c9e549
4        1   /Boot/cs-CZ/memtest.exe.mui ca2528f338b82dd551a656df2ae24f0f9cf2c31e
5        1   /Boot/da-DK/bootmgr.exe.mui bdc45ce9e6a1250f36dc0e2ebb8e56cb1bfbc108
6        1   /Boot/da-DK/memtest.exe.mui afcca1b897efbedbda75c8cf525cadf0abb147dd
7        1   /Boot/de-DE/bootmgr.exe.mui 404563c6f81f23f6965fe236b15b621496a48656
8        1   /Boot/de-DE/memtest.exe.mui fb95a556139bb6cee6fc5ee7002f2cd0b1ea9ac5
9        1   /Boot/el-GR/bootmgr.exe.mui 40a16ad142fdbc2801b4fc9288a152bcfa56a728
10       1   /Boot/el-GR/memtest.exe.mui 87187933da28d4ffe72bdfe5af0d42da3c287842
11       1   /Boot/en-GB/bootmgr.exe.mui 68fa4b6cbf452f3792964e61d7de6abe669ac989
12       1   /Boot/en-US/bootmgr.exe.mui b47ce7cc3c7bcbcab5f3222434a2123de5e478c8
13       1   /Boot/en-US/memtest.exe.mui fb348786d790fab2b24d266314e10e25798d8a7e
14       1   /Boot/es-ES/bootmgr.exe.mui 453cf611306ea98e0b38653a50f2c57df881dc86
15       1   /Boot/es-ES/memtest.exe.mui 0f36122e3694f5d9e74f7a05e1a3c475b937e623
16       1   /Boot/es-MX/bootmgr.exe.mui e3b3b15d1987029c32fa6dcabef681e0fb097ae7
17       1   /Boot/et-EE/bootmgr.exe.mui 600c449a72b3be703099257a020f025078bc12d7
18       1   /Boot/fi-FI/bootmgr.exe.mui 725bbce8ca6a24cbe51963cf510a5d7653ae9e59
19       1   /Boot/fi-FI/memtest.exe.mui d7501dd285c339e8710ad0f566f1065db49dfee8
20       1   /Boot/fr-CA/bootmgr.exe.mui 27caa18b6bbeb1addcca61c7fe59c6d941629e8f
21       1   /Boot/fr-FR/bootmgr.exe.mui a8021cd46053102aa6e6ff4ebde5f9ed7759db5e
22       1   /Boot/fr-FR/memtest.exe.mui 2f0b2455d56f2ae004b19fa0111f5e5001823d9c
23       1   /Boot/hr-HR/bootmgr.exe.mui b34252ff49644fed39baa8dd708b06555f8cc938
24       1   /Boot/hu-HU/bootmgr.exe.mui b296f984ca0e732f11c5e4f5a4550d99d8ca7431
25       1   /Boot/hu-HU/memtest.exe.mui 6b55844a78498c3cea2888cdcf86da58e0e6b09a
```

When full protection mode is started all hashes are collected.
Non-authorized processes are blocked.



Mode Configuration

Please select a hash calculation mode. If this is the first time the VM has been put in full protection mode, full hash calculation must be performed.

○ Calculate hashes for all modules

Hash calculation is performed for all modules on Guest OS. To start **Full Protection Mode** for the **first time**, full hash calculation must be performed. This process is performed asynchronously, so users can continue working.
Note: This may take up to 50 minutes.

● Calculate hashes only for specified modules

Hash calculation is only performed for modules specified in the XML input file. An XML file that conforms to the schema specified in the document is required.
Note: The hash for any module that was modified must be recalculated, otherwise the module cannot be executed.

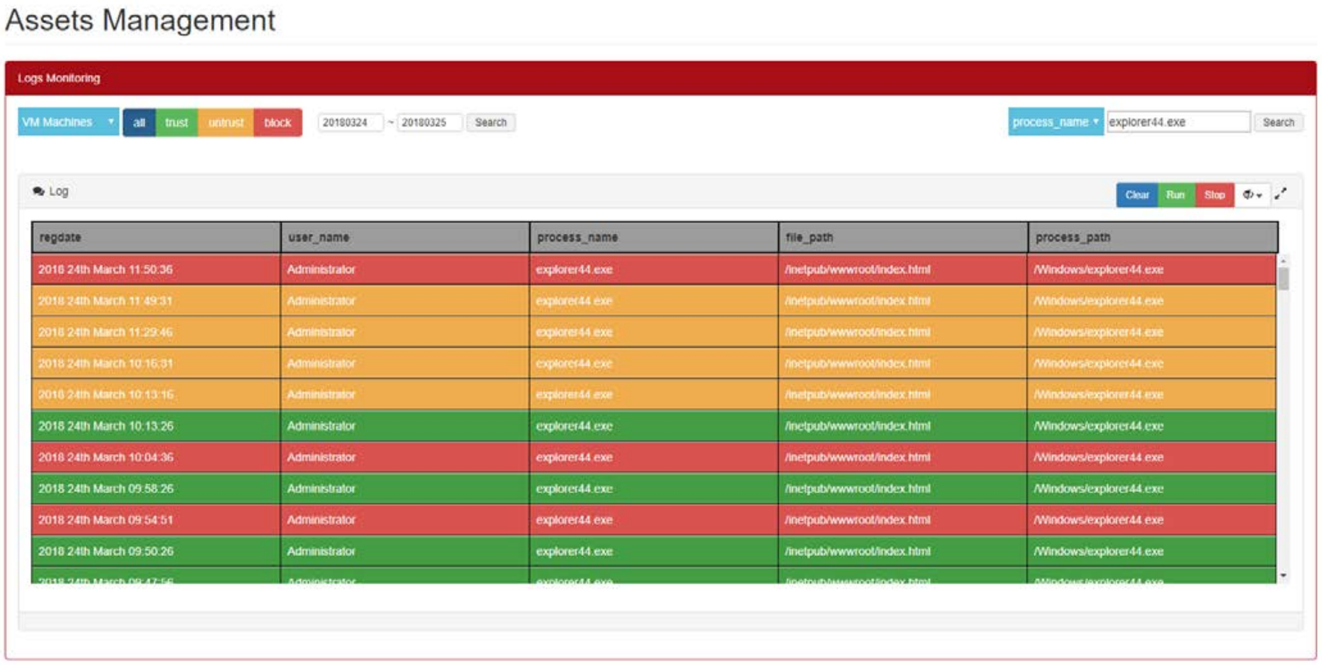
/home/joshua/Documents/ered-win10-vol.xml

○ No hash calculation

Hash values will not be recalculated. Current hash values will be retained.
Note: Hash vavlues must match, otherwise VM may fail to start.

Update hashes and allowed applications in Update Mode.
*eReD can be updated seperately in Maintenance Mode.

03 Logging / Monitoring



Assets Management

Logs Monitoring

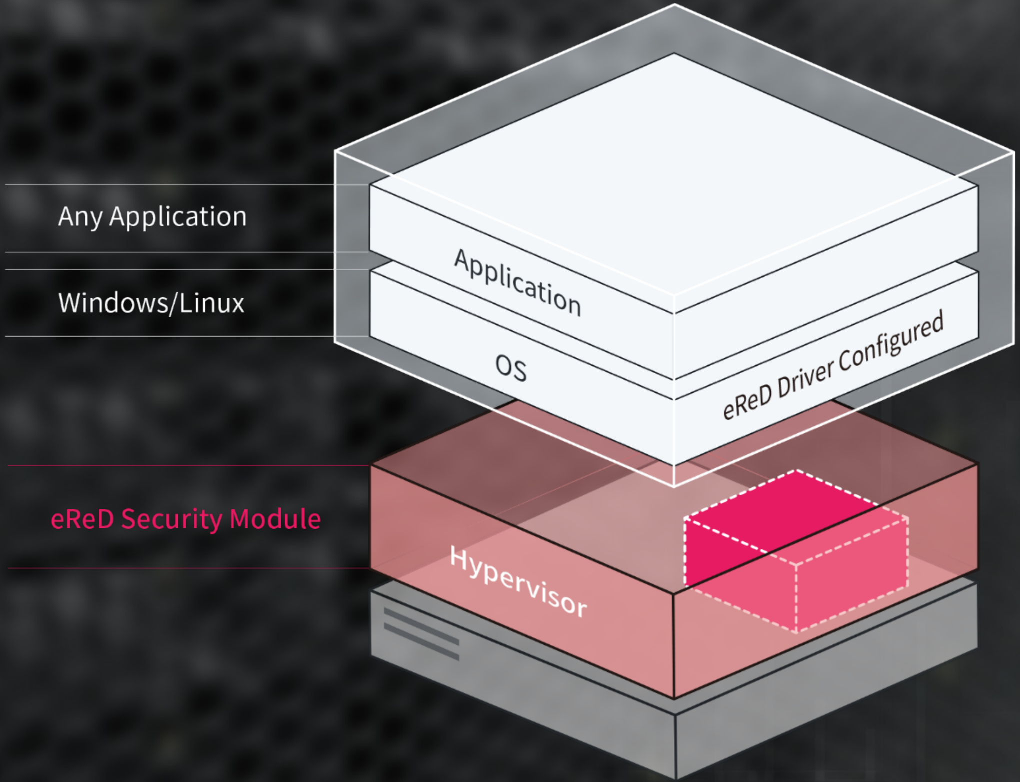
20180324 ~ 20180325

process_name: explorer44.exe

regdate	user_name	process_name	file_path	process_path
2018 24th March 11:50:36	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 11:49:31	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 11:29:46	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 10:16:31	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 10:13:16	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 10:13:26	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 10:04:36	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 09:58:26	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 09:54:51	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 09:50:26	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe
2018 24th March 09:47:56	Administrator	explorer44.exe	/inetpub/wwwroot/index.html	/Windows/explorer44.exe

- Immediately recognize and respond to security threats using eReD's real time logging
- Intuitively understand and analyze the log with the variety of statistics eReD provides.

eReD HYPERVISOR SECURITY Product structure



Guest Environment (VM Support)

Supported OSs

- Windows Server: 2016, 2012 (R1/R2), 2008 (R1/R2)
- Windows: 10, 8, 7, XP
- Linux: Coming Winter 2018

Supported Server Applications

- Web Servers: Apache, IIS, etc.
- Web Application Servers (WAS): Tomcat, Web Logic, Web Sphere, Zeus, Jboss, etc.
- DB Servers: MS-SQL, MySQL, PostgreSQL, etc.
- Data Backup Server

Host system requirement

CPU

- Intel processor with VT-x, AMD processor with AMD-V (x86)

OS

- Ubuntu 16.04

Where can eReD be used?

Industrial security server/private cloud

Applications: Cold Wallet Servers, Web Servers, Data Servers, Personal Information Management Servers, Backup Servers, Patch Servers, etc.

Issues

- A growing number of new and variant malware are increasing server infection and data exfiltration rates
- Ransomware that encrypts files and demands a ransom.
- Data exfiltration by internal users can cause serious damage.
- An infected patch server contaminates entire systems or backup servers, rendering them irrecoverable.

With eReD

- Completely block malware/ransomware from executing
- Apply policies to prevent the exfiltration, tampering, or damage of important data.
- Protect your server even with the admin or root account is compromised.

Manage Work Processes

Blocks Unauthorized Applications

Protects Files by Policies

Prevents Data Exfiltration and Tampering

Security Can't be Disabled (Self Protection)

Blocks Malware

Where can eReD be used?

Secure PCs for Special Purposes

Applications: Industry Control Systems, Infrastructure Services (Transport, Health, etc.), Management Ops, Remote Terminals, etc.

Issues

- Increasing cyber threats against critical national infrastructure
- control systems
- Even closed networks have vulnerabilities like the admin PC.
- Using system vulnerabilities unauthorized personnel may circumvent access control to access to important data.

With eReD

- Completely block unauthorized applications from running on the admin PC to avoid infection.
- Only trusted applications are permitted to run
- File access control done in the hypervisor, so it cannot be bypassed or disabled..

Manage Work Processes

Blocks Malware and Unauthorized Applications

Prevents Data Exfiltration and Tampering

Security Can't be Disabled (Self Protection)

USB and External Hard Disk Access Blocking

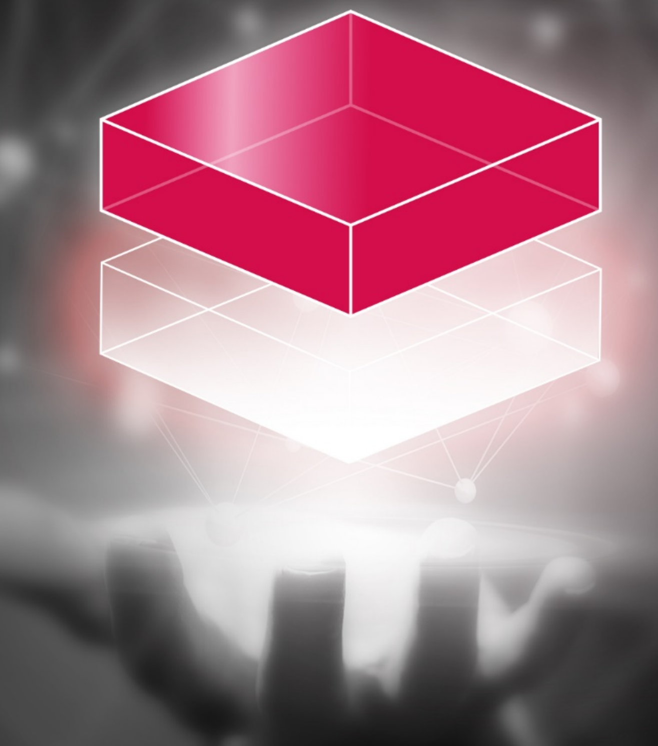
Logs File Access/ Execution and Blocking Actions

eReD Security Testing Results

eReD has been verified by 3rd party whitehat hacking organization. The results show that eReD protected against all attempted attacks on the report. For industrial control system that demand tight security, eReD is up to the task.

Reference: 'Whitehat Hacking Report for the Hypervisor Based Web Source Security Solution (2017/11/20-2017/12/19)'.

Attack scenario	Result
Gain Administrator Privileges	
Executable malware (file executables – 12 scenarios) (dll injection, api hooking, etc.)	Defense success
System Boot Record Attack	
Attacks against disk record volumes including MBR, VBR, etc. (2 scenarios)	Defense success
Disable eReD Self Protection	
Attacks against memory, binary, driver, registries, etc. to tamper with and delete the guest agent (4 scenarios).	Defense success



The old era is over. Welcome to the new era.

Now with eReD