Security Solution

WIDGET
OBSERVER

RANSOM
DEFENSE

SOFT
FILTER

WidgetNuri

01 Widget Observer

Widget Observer

Widget Observer is a security solution that increases the efficiency of your business by monitoring and controlling the process of abnormal operation of your PC and protecting your PC from illegal and malicious software.

Process abnormal behavior analysis and monitoring

Process I/O, Network control

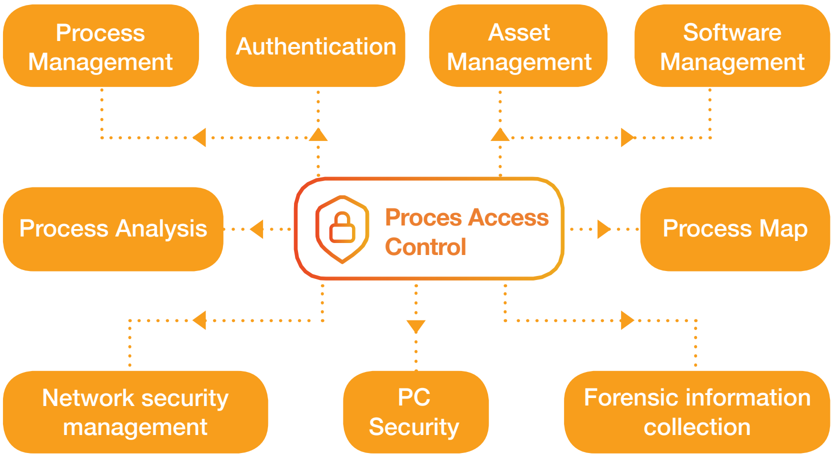
Increase work efficiency

WIDGET OBSERVER

Introduction Effect

Processes can monitor abnormal behavior through thresholds and growth rates such as I/O and network traffic, and utilize various security data as data for digital forensics through collection and analysis.
In addition, powerful process-specific controls block only problematic processes and do not impact your business. You can manage software safely through various policies and collections related to processes.

Main Function



Features

- Blocking by processes that do not interfere with work
- Comfortable work environment support
- Ensuring the integrity of your PC
- Powerful network management
- Detect critical equipment access processes
- Process access tracking using IP/PORT
- Process communication correlation analysis
- Various data collection and analysis

02 Ransom Defense

Ransom Defense

It is a security solution that protects the user's PC by blocking against the newly developed Ransomware and the newly developed new / variant Ransomware based on the intelligent whitelist.

Software Authentication

- Verifying Unknown Software Reliability
- Verifying data integrity and information reliability
- Proactive blocking of new/variant Ransomware
- Normal Software Automatic Authentication

Intelligent Whitelist

- Whitelist through software authentication
- Auto update whitelist
- Convenient whitelist management
- Unknown Ransomware Diffusion Prevention

RANSOM DEFENSE

Introduction Effect

Existing security measures limit the protection of critical documents from the risk of ever-evolving Ransomware. Ransom Defense, based on an intelligent whitelist based on software authentication rather than traditional blacklist-based security, can be safe from the threat of Ransomware.

Main Function

Software Authentication	· Software Reliability Check · White / Gray / Blacklist Auto Registration
List Management	· Easy management of white / gray / black list
Behavioral Monitoring	· Ransomware of behavior monitoring · Abnormal process file access blocking
Process I/O Threshold Control	· DLL injection and script blocking · Block abnormal process file access thresholds · Complementing the limits of behavior-based
Back-UP	· Automated backup of critical data · Recoverable when critical data is damaged
Folder protection	· Custom Folder Strong Protection · Not all software can be accessed · Ability to manage designated folder

Features

Software Authentication
- Only authorized software can access critical data
- Reliability verification through various software analysis

Protect important documents
- Behavioral Monitoring and blocking
- Detect and block file tampering monitoring

Whitelist-based
- New/Variable Ransomware Available for Initial Response
- Sharing and managing authenticated software

RANSOM DEFENSE

How it works

**Critical Data Corruption +
Threat of Variant Behavior**

STEP 1	Software Authentication	· Software automatic analysis · Block unauthorized software execution · Automatically update white / gray / blacklist results
STEP 2	Behavioral Monitoring	· 1-Step Verified Software Activity Monitoring · Ransomware suspicious behavioral monitoring and blocking · Behavior based supplementation through threshold control
STEP 3	Real-Time Data Protection	· Ransomware protects and restores data in case of suspicious activity · Protect your data with custom protected folders

System Requirements

Policy Server	
OS	Linux CentOS 7
CPU	Intel ® Xeon 5600 higher
Memory	8GB higher
HDD	500GB higher
Administrator console	Web browser
Agent	
OS	Windows 7 (32/64bit) higher
CPU	Intel ® Core i3 3.1GHz higher
Memory	4GB higher
HDD	100GB higher

03 Soft Filter

Soft Filter

As new malicious activity increases day by day, we need an automated, intelligent whitelist to authenticate normal software. The SoftFilter solution allows the software to be analyzed and diagnosed and authenticated in a variety of ways. In addition, you can automatically block illegal, malicious, or unidentified software.

Features

- Only normal software can run
- Works without whitelist database
- Software updates can be automatically authenticated
- Easily add to any security system
- Manage software

GOOD Software

특허청

nuri

W

WidgetNuri

☎ 82 2 2043 8292

✉ qna@widgetnuri.com

🌐 www.widgetnuri.com