# ClearSkies™ NG Endpoint Detection & Response (EDR)

# Agent Version 6.1

**Incorporating the power of**

**Big Data Advanced Security Analytics**

**June 2019**

# Release Notes

# Table of Contents

## Overview

ClearSkies™ NG EDR Agent v6.1 is a comprehensive Endpoint Detection & Response solution, fully integrated with ClearSkies™ SaaS NG SIEM. It complements the detection and prevention of never-before-seen targeted attacks and insider threats with the use of Behavioral Monitoring and Analysis (BMA) and by leveraging Advanced Security Analytics complemented by Threat Intelligence and signature-based detection.

## What's New in v6.1:

- Next-Gen Behavioral Monitoring and Analysis
- Integrated Threat Intelligence
- Application Control
- Automated Response Actions

## New features

Several major new features and enhancements are introduced in this new **ClearSkies™ NG Endpoint Detection & Response (EDR) Agent** version 6.1:

### Automated Response Actions

*Simulated block*

The Agent can be configured to conduct a simulated block of suspicious events/activities that may be judged as normal in the individual use context.

*Block*

The Agent effectively blocks events that have been verified as malicious before they actually occur.

*Quarantine*

The Agent isolates events verified as malicious in a protected location on the endpoint. These malicious events can be reviewed at any time in the ClearSkies™ NG EDR "Vault" panel of the Agent's system tray, or by accessing the "Endpoint" Service Module of the ClearSkies™ Secure Web Portal.

**Automated actions and responses per activity**

| TYPE OF ACTIVITY | ACTION | RESPONSE |
|---|---|---|
| **Suspicious** | Simulated Block | Alert<br>or<br>Alert & Incident |
| **Malicious** | Simulated Block<br>Block<br>Quarantine | Alert<br>or<br>Alert & Incident |

### Signature-Based Analysis

- The Agent complements the detection and prevention of never-before-seen targeted attacks and insider threats with the use of Behavioral Monitoring and Analysis (BMA) and by leveraging Advanced Security Analytics complemented by Threat Intelligence and signature-based detection.

### Application Control

- The Agent grants full control over which applications on critical workstations and servers may run or not. This handy feature eliminates unknown/undesirable applications on your hosts that may compromise security and impact resource availability.

### Operational Status and Configuration Interface

- The Agent includes a system tray (or "systray") icon found on the Microsoft Windows operating system environments taskbar, which allows for the review of operational status and configuration parameters.

### Real-Time Visibility of Suspicious and/or Malicious Activities

- With the use of Windows notifications, the Agent informs endpoint users in a case of detection of malicious and/or suspicious activities on the endpoint.

# Enhancements

## New Log Sources Supported

### *Microsoft DNS logs client/server*

- Supports the collection and analysis of Windows DNS logs, either from Windows Servers or Clients, in order to identify suspicious activities including communication with malware/botnet domains.

### *W3C logs*

- Supports the collection and analysis of W3C access log and event data containing information about web access request, including the source Internet Protocol (IP) address, the HTTP version, the browser type, the referrer page, and the timestamp for supported Web servers.

## Enhanced Reporting Capabilities

- New fields are available for reporting, providing the ability to generate reports tailored to your business needs.

## Online and Offline Protection

- Continuously monitors and responds against never-before-seen attacks for incident remediation and non-intrusive user experience even when endpoints are taken offline.

## Behavioral Monitoring & Analysis (Watchdog)

- Analyzes in real time running processes for the detection and prevention of never-before-seen attacks like Malware, 0-day exploits and APTs as they emerge, drastically reducing workloads and all related costs as a result.

## Built-In Threat Intelligence

- Accelerates the detection of and response to emerging threats and vulnerabilities with the integration of various Threat Intelligence feeds, presented in the form of Indicators Of Compromise (IoC).

## User & Entity Behavior Analysis (UEBA)

- Profiles user-related host/network/application activities for the purpose of detecting suspicious/malicious behavior and intrusions, by identifying meaningful anomalies or deviations from “normal” patterns of behavior.

## Bug Fixes

This version resolves a number of stability and performance issues identified.

# Previous Versions Highlights

## Version 6.0.2

- Support for SWIFT Alliance Entry.
- LogFile Forwarder support for compressed files. File Types supported: AR, ARJ, CAB, CHM, CPIO, CramFS, DMG, EXT, FAT, GPT, GZip, HFS, IHEX, ISO, LZH, LZMA, MBR, MSI, NSIS, NTFS, QCOW2, RAR, RPM, SquashFS, UDF, UEFI, VDI, VHD, VMDK, WIM, XAR, Z, Zip.
- Performance fixes and improvements.

## Version 6.0.3

- Support for OSI Soft Pi Historian.