DATA SHEET

ClearSkies™ Endpoint

Detection & Response (EDR)

ClearSkies™

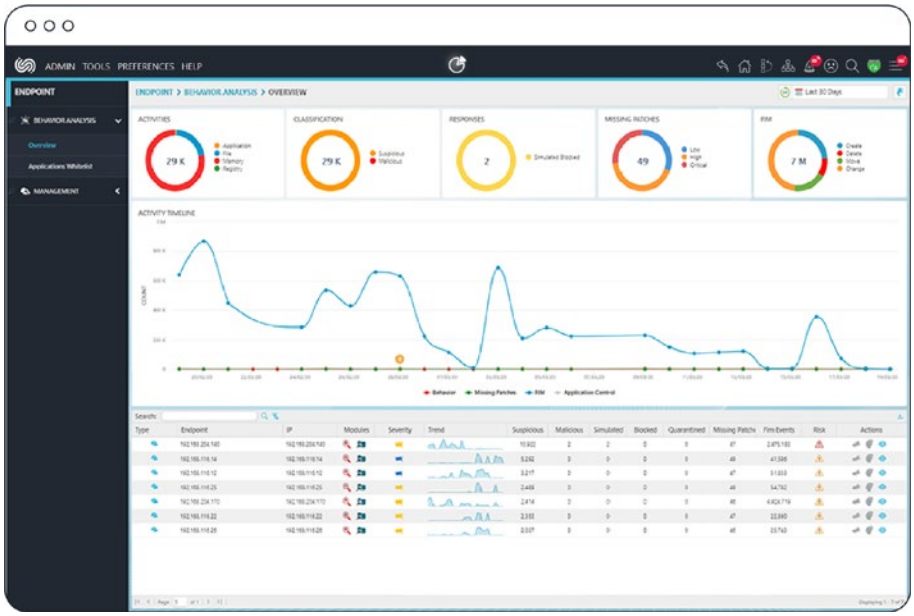
What is Endpoint Security

Endpoints are still the weakest link to your organizational network

ClearSkies™ Endpoint Detection and Response (EDR) is a comprehensive Endpoint Protection solution, fully integrated with ClearSkies™ Cloud SIEM. It complements the detection and response of cyber, insider and third-party threats by utilizing Behavioral Monitoring and Analysis (BMA), which leverages ClearSkies™ advanced security analytics, and Threat Intelligence.

Deploy ClearSkies™ Endpoint Detection & Response (EDR) on your critical workstations and servers, either on-premises or in the cloud for your Endpoint Security needs.

Today's sophisticated information-threats require more than traditional antivirus protection.



ClearSkies™ Endpoint Detection & Response (EDR) complements the detection and response capability of ClearSkies™ Cloud SIEM, delivering enhanced visibility over your organizational security posture.

What it does

An Endpoint Security solution to help detect and stop suspicious/ malicious activities and user abnormal behaviors by using Behavioral Analysis together combined with File Integrity Monitoring (FIM).

- **Get real-time visibility for faster response**
- **Automate and orchestrate response actions**
- **Prevent data leakage**
- **Simplify Incident Investigation and Threat Hunting**
- **Identify users' suspicious/malicious behaviors by using UEBA**
- **Enhance and simplify compliance and auditing requirements**

EDR as easy as A-B-C

- No security expertise required
- Deploy & manage easily
- No performance degradation

What you get

Security Automation and Orchestration

Capitalize on early detection, orchestration and response automation capabilities that reduce the time and resources needed to analyze and manage security events.

Online and Offline Protection

Benefit from continuous monitoring and response against never-before-seen attacks for incident remediation and non-intrusive user experience even when endpoints are taken offline.

Protection Against Network Threats

Take advantage of comprehensive network activity monitoring using behavioral analysis, towards the effective response to potential threats.

Detection and Prevention of Malware, 0-day Exploits and APTs

Employ constant monitoring of the integrity of key system configuration files, key system files, critical files/folders and running processes, enabling the timely detection of and response to Malware, APTs and 0-day threats.

Advanced Security Analytics with Threat Intelligence and Signature-Based Detection

Maximize the effectiveness of your detection and prevention capabilities by leveraging Advanced Security Analytics, Threat Intelligence and signature-based detection.

Awareness of Who did What from Where and When

Audit and monitor access to user-defined critical files/folders for policy violations, which could lead to data leakage or corruption.

Compliance/Auditing

Effortlessly achieve and demonstrate mandatory regulatory requirements prescribed by PCI DSS, ISO 27001, SWIFT, HIPAA, FISMA and GDPR, in an efficient and cost-effective manner.

Real-Time Visibility

Leverage an easy-to-use, feature-rich and highly customizable graphical user interface, which provides real-time visibility of your security posture, helping you with your decision-making process when strategically planning your internal defenses against emerging threats and vulnerabilities.

Accelerated Return On Investment (ROI) and Immediate Results

Reap the benefits of Endpoint Security and resilience immediately, without security expertise or setup administration costs.

Cutting-Edge Features

Bolster your Information Security Arsenal with Top-Notch Features:

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.

User & Entity Behavior Analysis (UEBA)

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

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 (IOCs).

File Integrity Monitoring (FIM)

Tracks privileged users’ access activity, including content modifications changes, for user-defined sensitive critical files/folders by account name and process, and when those files/folders were Accessed, Created, Viewed, Modified or Deleted.

Application Control

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.

YARA Rules

Contributes, through out-of-the-box packaged and ready-made rules, to early detection and response capabilities, based on contextual and binary patterns of threat behavior as it relates to malware families.

Contact Us

Cyprus (Headquarters)

1 Lefkos Anastasiades Str. 2012
Strovolos, Nicosia

T +357 22 463600
E info@clearskiessa.com

www.clearskiessa.com

OFFICES CYPRUS | GREECE | USA | UK | KSA