EDR - Endpoint Detection & Response
Unified Endpoint Security

ENDPOINTS ARE STILL THE WEAKEST LINK TO YOUR ORGANIZATIONAL NETWORK

The cybersecurity threat landscape is always expanding as cyber-attacks are becoming more and more complex and intuitive. Adversaries devise more intricate ways to breach through your organization's defences to target your workstations, networks and compromise your sensitive data. While many organizations try to address these with various solutions these are often disparate. They lack a unified approach, as data collection and analysis is out of context, leaving security teams to stumble blindly in the dark during incident remediation. Add to that, the impossible task of security teams trying to predict every possible threat and vulnerability that has yet to emerge.

ClearSkies™ EDR

ClearSkies™ Endpoint Detection & Response (EDR) provides unified visibility of your endpoints, complementing the early **detection**, **prevention** and **automated response** to targeted attacks and insider threats through powerful analytics. With ClearSkies™ EDR, security teams can have end-to-end visibility across all security levels and a stack of intuitive tools that enables to identify, analyse and respond to threat actors, even as they emerge.

Fully integrated with ClearSkies™ Threat & Vulnerability Platform, ClearSkies™ Endpoint Detection & Response (EDR) Agent can be deployed on your critical workstations and servers, either on-premises or in the cloud. Utilizing Behavioral Monitoring and Analysis (BMA), File Integrity Monitoring (FIM) which leverage ClearSkies™ advanced security analytics, and Threat Intelligence to audit all critical file systems provide proof of regulatory compliance.

KEY BENEFITS

Respond to and contain threats faster with real-time endpoint visibility, even remotely

Reduce your Mean Time To Respond (MTTR) by orchestrating and automating actions

Catch insider threats and suspicious users with User & Entity Behavior Analysis (UEBA)

Simplify Incident Investigation and Threat Hunting

Enhance and simplify compliance and auditing requirements with File Integrity Monitoring (FIM)

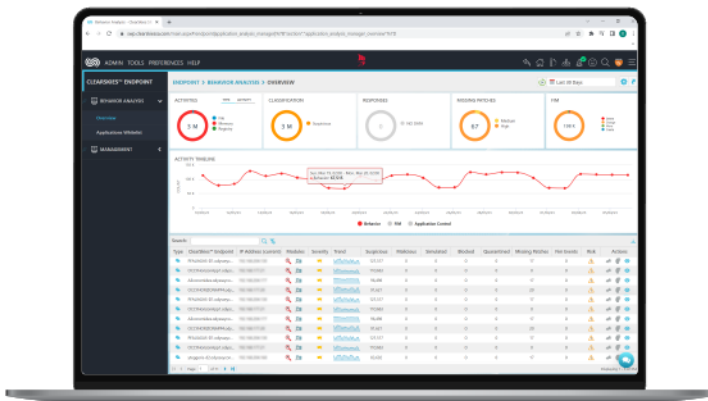Stay up to date with endpoint critical security updates

Monitor endpoint activity with minimal background requirements

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

DETECT & RESPOND TO ADVANCED ENDPOINT THREATS FASTER WITH ENHANCED TELEMETRY

Early Detection and Identification of Suspicious Behaviour in Endpoints

By collecting and analyzing billions of events from all applications, suspicious behavior in endpoints can be detected and identified early. This includes monitoring online and offline behavioral activity and digital signatures, even on devices that are offline or operate remotely.

Clearskies Endpoint, Behavior Analysis, Overview

Network Monitoring for Threat Activity

Network monitoring is continuous, with the ability to monitor network connections and DNS queries for malicious IPs and domains. Missing security patches can be identified based on the correlation between the endpoint operating system and affected CVEs.

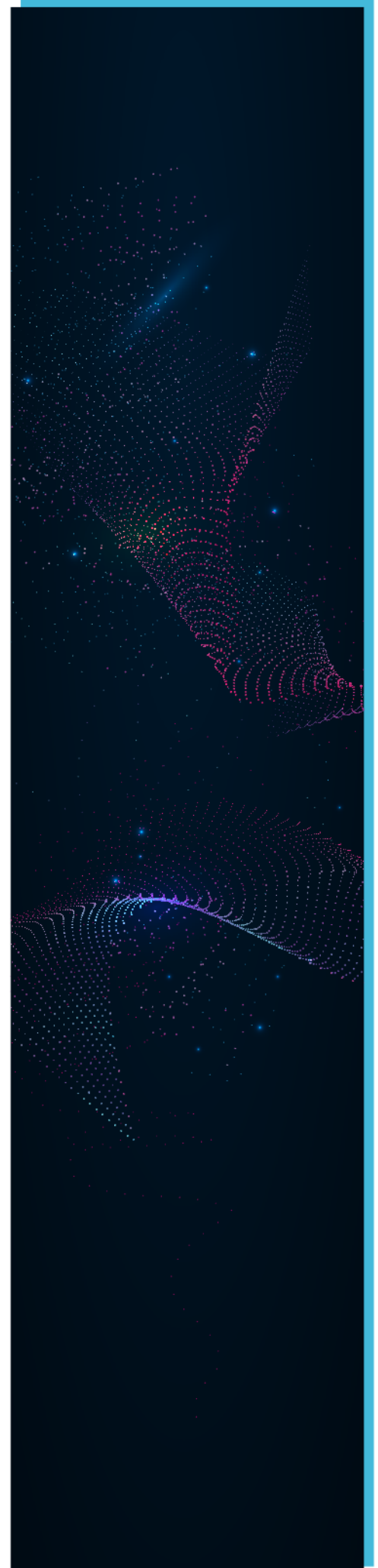## Unified Capabilities for Investigation and Remediation

ClearSkies™ EDR's unified capabilities extend to investigation and remediation, with the use of the Advanced Security Analytics engine and non-intrusive user experience of ClearSkies™ Threat & Vulnerability Platform. Threat issues can be investigated and/or automatically remediated.

Constant File Activity Audit

ClearSkies™ EDR's File Integrity Monitoring (FIM) allows for continuous audit and monitoring of access to key system configuration files, critical files/folders, and running processes.

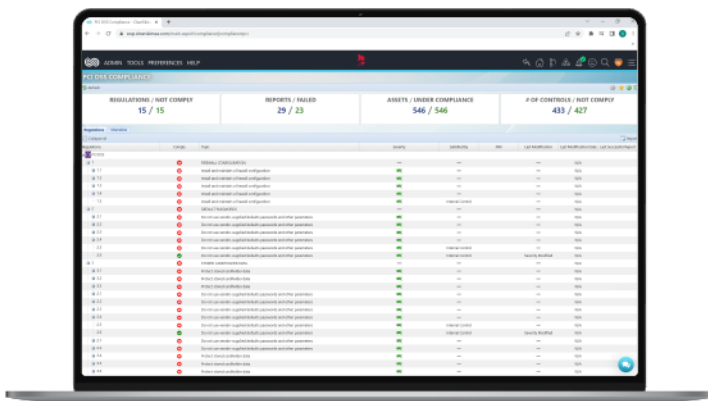Clearskies Endpoint, Behavior Analysis drilldown

Detection and Response to Threats

Combining FIM's constant monitoring with ClearSkies™ Threat & Vulnerability's powerful correlation and advanced analytics engine allows for timely detection, investigation, and response to Malware, APTs, and 0-day threats.

Regulatory Compliance Simplification

ClearSkies™ EDR FIM and ClearSkies™ Threat & Vulnerability Management Platforms Compliance Reporting make it effortless to achieve and demonstrate mandatory regulatory requirements prescribed by PCI DSS, ISO 27001, SWIFT, HIPAA, FISMA, and GDPR.
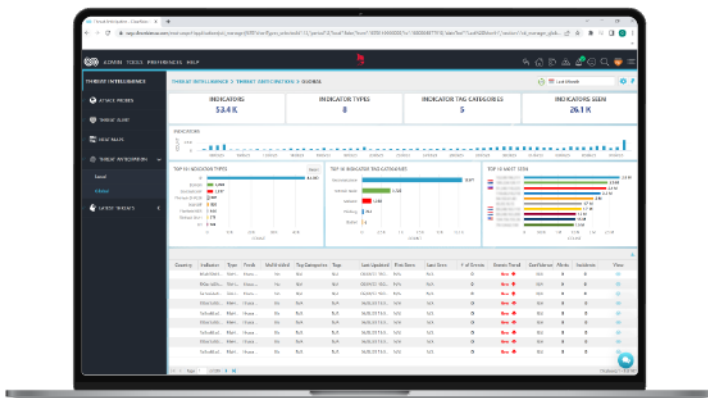

Compliance service module

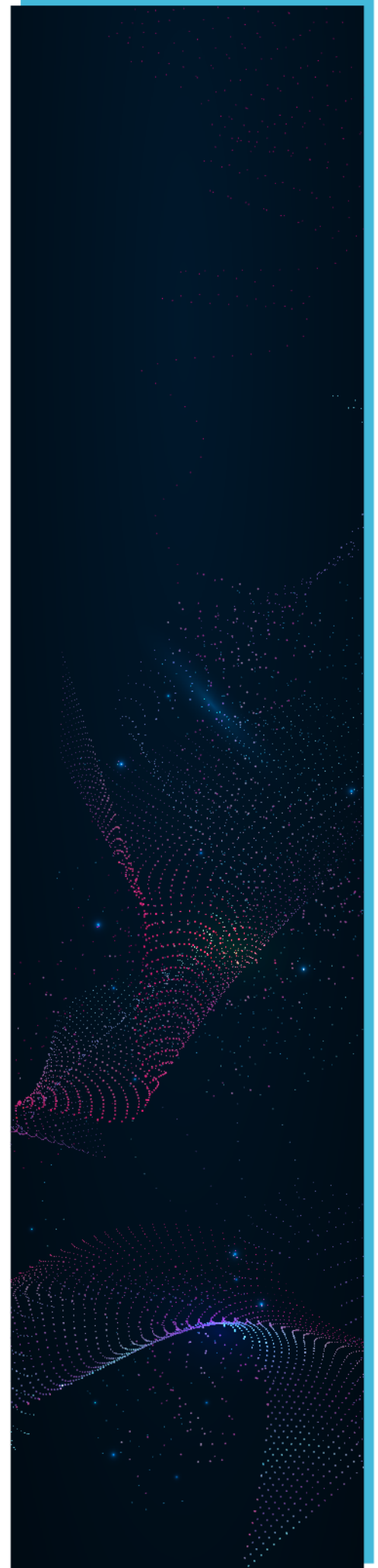## Automation and Orchestration of Detection and Response

ClearSkies™ SIEM Platform's SOAR capabilities allow for early detection, orchestration, and response automation. This reduces the time and resources needed to analyze and manage security events.

Automatic Synchronization of Threat Intelligence

ClearSkies™ EDR and SOAR automatically synchronize threat intelligence, updating the signature/security feeds in real-time to include all new threat information worldwide. This helps identify and include the latest malicious behavior/malicious IPs, checksums, and malware.

Clearskies Threat Intelligence, Threat Anticipation

CUTTING-EDGE FEATURES

- Behavioral Monitoring & Analysis
- User & Entity Behavior Analysis (UEBA)
- Built-in Threat Intelligence
- File Integrity Monitoring (FIM) & Compliance
- Application Control
- YARA Rules
- Missing Security Patches Reporting
- DNS Traffic Monitoring

ENHANCE YOUR EDR PROTECTION WITH ClearSkies™ INTEGRATIONS

Further expand your detection and response capabilities by integrating the ClearSkies™ Add-On products:

Active Defense

Enhance your endpoint protection with post-breach technology that reduce attacker dwell time by deploying "fake" information that lure and occupy attackers while you gain time to take defensive measures.

Identity & Access

Gain visibility of who did what and when in your organization through the integration of ClearSkies™ Identity & Access that offers expansive overview and detection of potential malicious/suspicious insider threats.

REQUEST A DEMO

ABOUT CLEARSKIES

Behind the creation and delivery of the award-winning ClearSkies™ Threat & Vulnerability Management Platform, is Odyssey. Odyssey is a leader in helping organizations globally manage their Digital Risks and meet Legal and Regulatory Compliance Requirements by fostering cyber resilience. The ClearSkies™ Threat & Vulnerability Management Platform empowers organizations to anticipate, respond to, swiftly recover from, and adapt to cyber, insider and third-party threats. The ClearSkies™ team inherits the tacit knowledge and holistic experience of tried-and-tested experts specializing solely in Cybersecurity solutions and services.

Cyprus (HQ) | Greece | MENA | UK

Learn more at **www.clearskiessa.com**