INFINITY

PROTECT EDR
Service Description
Hosted Endpoint Protection

INGRAM MICRO CLOUD MARKET PLACE

Last Updated: March 2021

 1-877-591-6711

 isacybersecurity.com

 infinity@isacybersecurity.com

PROTECT EDR Service Description

Overview

PROTECT EDR is a Hosted Endpoint Protection and Endpoint Detection and Response (EDR) Service. It is the critical last line of defense in protecting user devices from malicious attacks and keeping the data stored on those devices safe. ISA offers this service, tailored to meet your organizations needs and budget. Our offering includes:

1. **Hosted Endpoint Protection**: An advanced antivirus protection with a complete set of features for scanning, analyzing, blocking, and reporting in real time. Features include:

    - Endpoint Security Protection
    - Endpoint Security Firewall
    - Endpoint Security Web Control
    - Endpoint Security Advanced Threat Protection

2. **Hosted EDR**: Includes features to augment visibility for detecting and investigating suspicious activities (and traces of such), and other problems on hosts/endpoints. EDR works by monitoring endpoint and network events and recording the information in a central database where further analysis, detection, investigation, reporting, and alerting take place in our platform. Among its capabilities are:

    - Data search and investigations
    - Suspicious activity detection
    - Data exploration
    - Containment/Isolation

3. **Hosted Threat Hunting**: ISA's Hosted Threat Hunting leverages a Malware Analysis Platform that supports advanced hunting and investigations through high-speed automated static analysis. It is integrated with file reputation services to provide in-depth rich context and threat classification on over 8 billion files including all file types. We have access to threat intelligence dedicated database for malware search, global and local YARA rules matching, as well as integration with third-party sandbox tools.

4. **Hosted Sandboxing**: Our technology enables organizations to detect advanced, evasive malware and convert threat information into immediate action and protection. Unlike traditional sandboxes, it includes additional inspection capabilities that broaden detection and expose evasive threats. Tight integration between security solutions - from network and endpoint to investigation - enables instant sharing of threat information across the environment, enhancing protection and investigation. Flexible deployment options support every network.

Our Approach

ISA leverages our state of the art, SOC 2 Certified, Cybersecurity Intelligence and Operations Centre (CIOC) to deliver PROTECT EDR services 24/7 by 365. ISA provides a cloud security platform for endpoints to be monitored around the clock by different teams and to be tuned on a regular basis to deliver high-class service for our managed clients. Prior to onboarding, the CIOC Team designates an analyst to work closely with the client to collect and assess pertinent information and fully understand their priorities and concerns to provide a smooth experience and compatibility. Once, the initial information is collected, analyzed, processed, and vetted, the client will be provided with a specific agent, (software) to be installed on its endpoints to initiate protection and management. As new information is gathered, and as new threats are discovered, the environment is fine tuned to ensure the highest levels of protection are in place.

Deliverables and Outcomes

ISA's PROTECT EDR offering provides:

- 100% in house cloud solution providing reliability, resiliency, and accessibility
- A full stack of protection for endpoints
- Seamless integration of agents onto endpoints
- A highly trained and skilled team of cybersecurity professionals monitoring and alerting 24/7 by 365
- A ticketing and tracking system with a user-friendly web interface
- Access to reporting through Customer Portal

Partner & Client Involvement

The partner or client installs the agent in the client's environment. This may include imaging or re-imaging existing or newly acquired endpoints including the deployment of related products. Ongoing communication with ISA team will ensure continuous enhancement of services based on new policies, procedures or images client may introduce.

Industry Trend

Employees are increasingly relying on mobile devices, home computers, laptops, and tablets to conduct company business. Any of these devices provide an entry point for malicious actors. According to Verizon's 2019 data breach report[1], majority of breaches happen due to exploitation of vulnerabilities and misconfigurations. The traditional enterprise network security perimeter is no longer sufficient to protect your data.

[1] https://enterprise.verizon.com/resources/reports/dbir/

PROTECT EDR Features and Deliverables

PROTECT EDR comes with a set of enterprise-grade features to provide a world-class endpoint protection service:

Features & Deliverables[2]	PROTECT EDR	Partner support required?
Onboarding Process		
Project Manager support	✓	Yes
Whitelisting of existing security controls	✓	
Deployment of single agent	✓	Yes
POC Test for environment compatibility	✓	Yes
Alerting & Incident Response		
Access to ISA ticketing portal	✓	
Alerting & Escalation via ISA ticketing system	✓	
Creating tickets in ISA ticketing system	✓	
Pre-defined remediation playbook response for specific critical event	✓	
Monitoring & response 24/7 by 365	✓	
Architecture		
Network Security Control enablement	✓	Yes
Service available as a Cloud Service	✓	
Canadian Data Sovereignty option	✓	
Reporting		
Access to Customer portal	✓	
Endpoint Protection		
Endpoint Security Protection	✓	
Endpoint Security Firewall	✓	
Endpoint Security Web Control	✓	
Endpoint Security Advanced Threat Protection	✓	
File Reputation	✓	
Zero Day Protection through Machine Learning	✓	
Zero Day Protection through Sandboxing	✓	
Endpoint Detection & Response		
Data search and investigations	✓	
Suspicious activity detection	✓	
Data exploration	✓	
Containment & Isolation	✓	
Threat Hunting	✓	

[2] Non-exhaustive list, subject to change

PROTECT EDR Pricelist

PROTECT EDR is priced monthly, per endpoint. For details, see the Ingram Micro Cloud Market Place.

ISA Difference

ISA's state of the art, SOC 2 Certified CIOC provides unparalleled security and availability. Constantly staying ahead of the latest threat is next to impossible (and cost prohibitive) for most organizations. We have nearly three decades of experience, dedicated staff, and clients from diverse industries and varying company sizes. As such, we have a large defence ecosystem, the use cases, and the deep expert knowledge needed to secure your business.

THIS SERVICE DESCRIPTION DOCUMENT, INCL. THE PRICELIST IS INTENDED EXCLUSIVELY FOR INFINITY PARTNERS, INFINITY PARTNERS CAN PRICE THE SERVICE FOR END CLIENTS AT THEIR DISCRETION