Infigo
Managed EDR

Superior security in a fast and cost-effective way

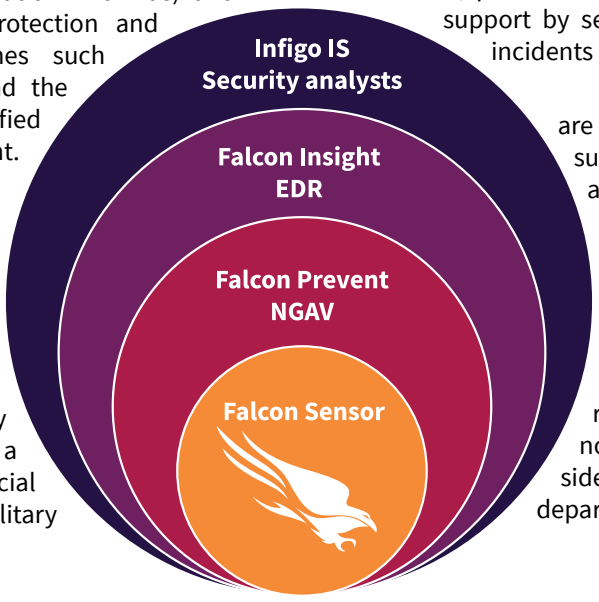
MANAGED ENDPOINT DETECTION AND RESPONSE

Small, medium or large, **organization of any size needs superior information security**. With the constant rise in malware, ransomware, phishing, and all kind of hacking attacks, **the question is when not if**, are malicious actors going to knock on your door. And it would be for the best that on the other side is **a team of trained security analysts with a world-class security platform**

Infigo Managed EDR (Endpoint Detection and Response) is a service intended for small, medium, and large organizations that want to have superior security at their endpoints (workstations, servers) at **a cost-effective price with high efficiency**. The service is based on **a combination of CrowdStrike Falcon and Infigo IS**' many years of experience in the world of information security (offensive and defensive side, implementation and consulting in often critical environments across Europe, Africa, and the Middle East).

CrowdStrike Falcon today is the best endpoint security platform that combines multiple modules such as Falcon Prevent (NGAV, Next Generation AntiVirus) and Falcon Insight (EDR, Endpoint Protection and Response); industry-leading names such as Gartner, Forrester, SE Labs and the like have for many years classified CrowdStrike as a leader in its segment.

Infigo IS has been involved in information security for more than 15 years - the offensive team performs more than 350 security tests a year, while the defensive team continuously monitors organizations on three continents. With a large number of security products implementations across a range of industries, from the financial sector through telecoms to military alliances, they are perfectly positioned not only to configure security solutions but also to proactively seek advanced threats which, unfortunately, are more and more common.



Two service levels – Standard and Enterprise

Infigo Managed EDR comes in two versions, Standard and Enterprise. Standard is a combination of a next-generation antivirus solution (**Falcon Prevent**) and additional security policy customizations, while Enterprise includes full EDR (**Falcon Insight** module) through advanced telemetry collection, proactive monitoring and incident resolution support by security analysts, and searching for incidents that evaded automated system.

In both versions security experts are in charge of agent deployment support, configuration of protection and detection policies with periodic updates, but in the Enterprise version, security analysts are proactively monitoring for incidents that slipped by Falcons automatic defenses, threat hunting, and supporting incident resolution. Security analysts do not do remediation on the client's side – that is a job for the internal IT department.

Who does what?

CROWDSTRIKE FALCON

CrowdStrike Falcon controls the endpoints (workstations, servers) and through advanced algorithms tries to **prevent malicious actions**. At the same time, it reports telemetry (records of all initiated processes, network connections, user authentication...) to the **cloud within the EU** and sends automated reports on successfully prevented security incidents.
The agents, Falcon Sensor, have **extremely low hardware requirements**; 50-75 MB RAM and CPU usage below 1 percent. They also have minimal network requirements - it needs only access to a defined list of URLs and IP addresses, to have access to the cloud console.

INFIGO IS

Infigo IS is in charge of CrowdStrike Sensor administration at the endpoints and every time Falcon fails to solve a problem, it jumps into action. As much as the CrowdStrike Falcon is an advanced security platform, it still has its limitations because it doesn't understand context, unlike security analysts. There is no software on the market that could offer steps to solve problems that it doesn't know how to deal with, for that an experienced analyst is needed. **While not dealing with current incidents, security analysts use telemetry to find patterns that point to an emerging security incident** (e.g., advanced attacks can take place through multiple steps that stretch over months to avoid detection) or some that have already occurred but were not detected.
The reports that Infigo IS submits upon detection of each incident that CrowdStrike Falcon could not deal with, **contain a detailed description (what happened, who was involved...) and recommendations** and steps on how to correct the problem.

THE CLIENT

The client receives automated reports straight from the CrowdStrike cloud, receives **individual incident reports** handled by Infigo IS, has **access to the cloud console** where they can monitor activities in real-time, and enjoys a mix of the best of both worlds - **CrowdStrike Falcon's ability to automatically prevent a large number of malicious actions and Infigo IS security analysts who solve all problems that the software cannot and proactively look for undetected incidents**. The client's IT department is still in charge of remediation within the client network with guidance by Infigo IS.

The whole **system is layered** – in every instance there will be a **Falcon Sensor, a lightweight agent** that is administrated through the cloud console, but has all the logic and machine learning capabilities in itself. That is why **CrowdStrike Falcon functions without a problem if it loses connection with the cloud**. There will always be security experts who will be in charge of administration and extra tuning. And there will always be Falcon Prevent, a next-generation antivirus solution that has great automatic prevention capabilities.
But **with Falcon Insight comes full EDR component** – advanced telemetry that enables security analysts to proactively search for advanced threats that can sneak by Falcon Prevent, and threat hunting for finding complex threats that are unfortunately more and more prevalent in a modern security landscape.

Key Features

Superior security

Thanks to the use of CrowdStrike Falcon, organizations get all the benefits of cloud-oriented architecture; CrowdStrike communicates via an agent on the local computer with the cloud, which performs tasks such as patching and local agent upgrades. Machine learning and indicators of attack (IOAs) protect local infrastructure from all types of unwanted activities. The IOA focuses on what the attacker is doing now, thus defending organizations from malicious acts that may never have been recorded before. Classic antivirus programs look to the past because they can only fight threats that have already happened to someone and have their "signatures," but CrowdStrike Falcon has no such flaws.

Fast and precise implementation

Infigo IS prepares installation packages and provides support when installing agents on the client infrastructure.
Not only does implementation have no impact on the day-to-day operation of the information system but complete provisioning is measured in man-hours, not days! In addition to the preparation of the package, Infigo IS also adjusts the detection and prevention security policies according to the best security practices that have been born from the years of operation in complex information systems. After implementation, each agent becomes a unit in itself and functions independently so that local users practically do not notice the change on their machines!

Low requirements and scalability

The agent, Falcon Sensor, located on the local computer is extremely modest in terms of hardware requirements. At a time when a regular Internet browser takes up gigabytes of RAM, the Sensor needs 50-75 megabytes and less than one percent of CPU time.
As such, the entire system is extremely scalable so there is virtually no difference between a few agents and a few thousand - using CrowdStrike Falcon does not require additional investment in the hardware of any kind.

Continuous support

Infigo IS takes on continuous support that includes managing and upgrading security policies, proactive (24/7/365) incident monitoring and detection, incident resolution support, periodic threat hunting activities, and more.
Supervision is performed by security analysts with many years of experience who hold certificates from recognized international security organizations. Today, because of their continuous training, Infigo IS' experts have over 130 certificates, and that number keeps growing almost daily.

REPORTS

Organizations receive alerts about detected malicious actions in real-time, and automated monthly service status reports that are easily understood and read by stakeholders outside the technical profession.

FIXED COST

Infigo Managed EDR is a service that has no variable or hidden costs; each organization pre-arranges the scope and price and can be confident in the financial construction from day one without fear of unexpected expenses.

Infigo Managed EDR features	Standard	Enterprise
Managed Endpoint Protection yearly subscription	✓	✓
Agent deployment support	✓	✓
Protection and detection policy configuration	✓	✓
Automated incident and detection notifications	✓	✓
Automated periodic reporting	✓	✓
Cloud console access	✓	✓
Periodic protection and detection policy update	✓	✓
Advanced telemetry collection from endpoints	-	✓
Proactive monitoring and support in incident resolution	-	✓
Threat hunting	-	✓

nearly 80% of senior IT employees and security leaders believe their companies **lack sufficient protection against cyber-attacks** despite increased IT security investments made in 2020

What happens next is up to you - let us make your life easier

INFIGO IS d.o.o.
Karlovačka 24a
10020 Zagreb
Croatia
+385 1 4662 700
www.infigo.hr

INFIGO IS d.o.o.
Zmaja od Bosne 14C
71000 Sarajevo
Bosnia and Herzigovina
+387 33 821 245
www.infigo.ba

INFIGO Software Design LLC
2902, Level 29, Marina Plaza
Dubai Marina, Dubai
PO Box 5000307
United Arab Emirates
+ 971 4 512 4081
www.infigo.ae

INFIGO IS d.o.o.
Rr. Bardhok Biba, Pll. Hodaj, Shk. A, Ap.8
Tirana
Albania
+355 42 42 16 33
www.infigo.al

INFIGO IS d.o.o.
Tivolska cesta 50
1000 Ljubljana
Slovenia
+386 1 777 89 00
www.infigo.si

INFIGO IS d.o.o.
Ul. Metodija Shatorov Sharlo br. 30/2-17
1000 Skopje
North Macedonia
+389 (0)2 3151 203
www.infigo.mk