LABYRINTH
Developed to stop advanced threats

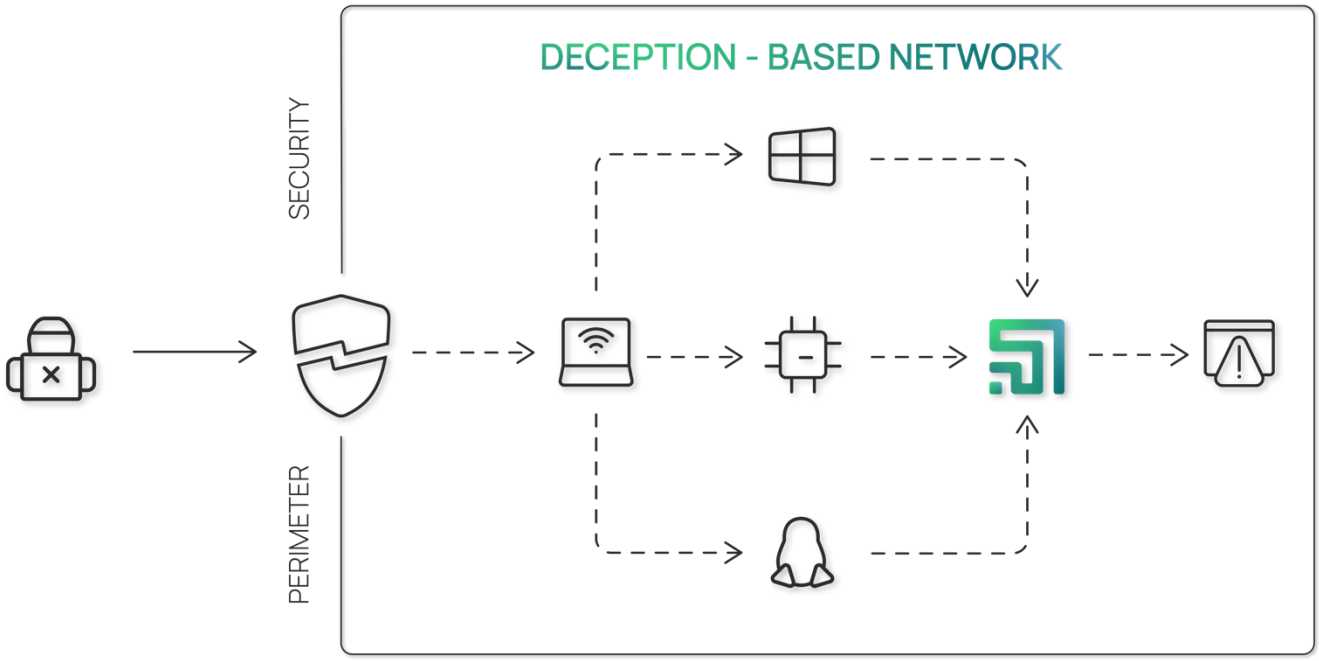
Solution Description

Labyrinth Deception Platform, 2023

Labyrinth is a deception-based threat detection technology that identifies and blocks cyber-attacks from within a corporate network. Powered by unique threat detection technologies, our solution proactively defends your network from targeted attacks, advanced unknown threats, botnets, zero-day attacks, and malicious insiders.

The platform provides a simple and efficient tool for the earliest possible detection of attackers inside an enterprise network. Easily deployed across virtual, physical, or hybrid IT environments, Labyrinth detects threats without continuous monitoring and producing tons of data.

The Platform provides a full attack timeline with events correlation to make smarter and faster decisions. Protection by Labyrinth is giving you peace of mind that your valuable data will remain protected against threats that have bypassed corporate firewalls.



KEY CAPABILITIES

There is a well-known asymmetry between attack and defense in the cyber security field: defenders need to be right 100% of the time, and attackers just need to be lucky once to succeed.

Labyrinth Deception Platform is an offensive detection technology that shifts the balance of power to defenders. The Platform eliminates an adversary's ability for network reconnaissance thus preventing lateral movement.

EARLY IN-NETWORK THREAT DETECTION

Labyrinth detects any targeted suspicious activity at the early stage of an attack. Labyrinth Points (network decoys) are designed to catch threat actions when an attacker tries to understand the network and to find its target. Once an attacker goes after a Point, Labyrinth gathers all the details about them: the threat sources, the tools used, and vulnerabilities exploited. At the same time, all real assets and services work without any impact.

ACCURATE ALERTS

Labyrinth supports security teams with highly reliable alerts with less than 1% false positives. By their nature, Labyrinth Points are silent until they are being touched. No one is supposed to contact them, so any interaction with a Point is exceptionally suspicious. This distinguishes Labyrinth from security solutions which are intended to analyze all activities in a network and produce a lot of digital "noise".

RAPID INCIDENT RESPONSE

Labyrinth provides an intelligent analytics instrument for incident investigation and threat identification. All gathered events are enriched with necessary security data from the Incident Response Platform.
Indicators of Compromise (IoC) generated by Labyrinth automatically synchronize to Threat Prevention Solutions. It allows immediately to take actions on attack: understand it, run the forensics on it, respond confidently and develop a better defense for the future.

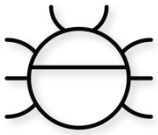
PROACTIVE DEFENSE

Most of detection technologies stop an attack once they have detected it and give no chance to study it. Important information, which helps eliminates an attack and prevents this attack from returning, is lost.
Labyrinth allows to learn more about an attack's nature and better understand tools and technics used by attackers. The solution generates and installs deception artifacts, whose aim is to engage attackers with a tempting fake. Instead of just waiting what an attacker's next step will be, the artifacts direct them to an isolated environment to be watched.

TARGETED ATTACKS UNCOVERING

To counteract effectively against targeted attacks, understanding of attackers' techniques, tools and goals is crucial.
Labyrinth Deception Platform lures hackers or malicious insiders into a false sense of security and allows them to learn their skillset and motives. Awareness of what attackers know about company networks, applications and employees helps to create the most accurate profile of attackers and apply the best possible way to defend against them. It also reveals weaknesses in corporate defense systems which can be exploited by adversaries in the future.

POST-INFECTION DETECTION

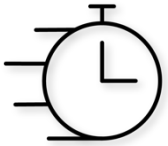


Labyrinth Deception Platform implemented within a company's networks can serve as a highly reliable alerting system of attacks that have bypassed perimeter security controls.
Seeder Agents, deployed on servers and workstations, mimic the most "delicious", for an attacker, artifacts. What appears to be a high-privilege and badly protected administrator account is a trap that entices an attacker to Labyrinth. There you can monitor attacker actions dealing with Points, gathering valuable insights about threats that have penetrated perimeter defenses.

LATERAL MOVEMENT RECOGNITION

In the phase of lateral movement, an attacker moves in a company network from one asset to another. Labyrinth Deception Platform is designed to detect early reconnaissance, credential theft, and lateral movement.
It allows companies to gain such threats visibility at their early stage that is a complicated task for traditional security solutions. Labyrinth directs the next step in an attack on the deception ecosystem and immediately reveals an attacker.

DWELL TIME REDUCTION



Labyrinth detection mechanism is especially efficient for reducing dwell time, which is a time when an attacker remains unnoticed inside a corporate network. Long dwell time is a crucial condition for an attacker to successfully complete an attack. Labyrinth shorten dwell times of attacks by setting up honeypots, decoys, and breadcrumbs for attackers. Labyrinth Deception Platform reduces the time and ability for attackers to move inside company networks and stops them before they reach critical assets and services.

BUSINESS VALUES

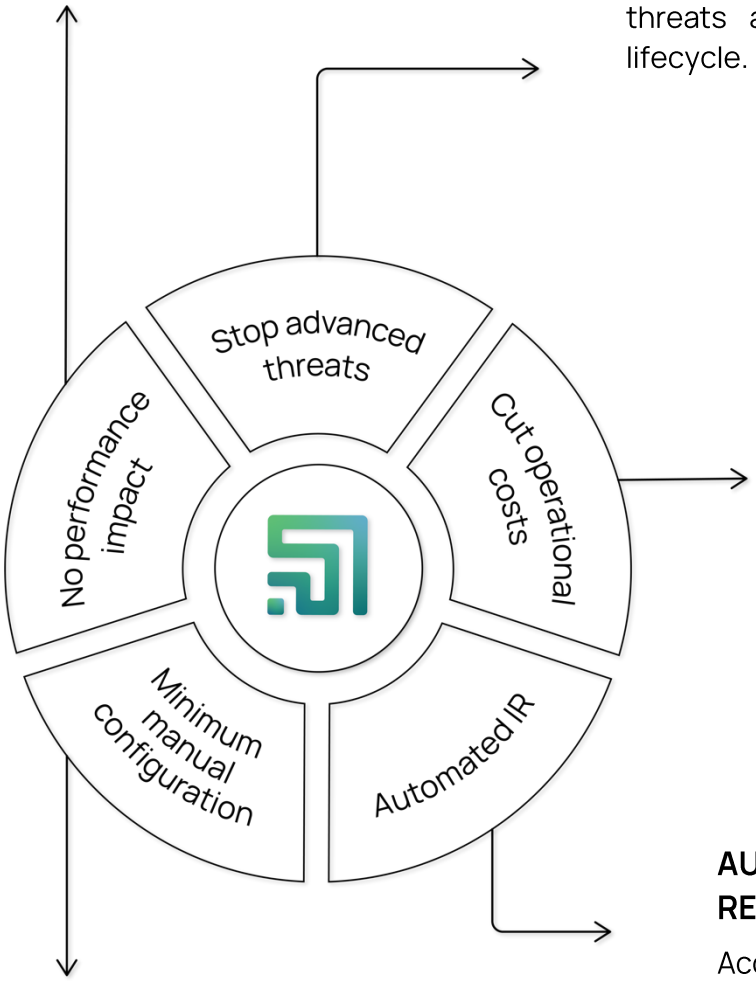
ZERO PERFORMANCE IMPACT

No negative impact on performance of network devices, hosts, servers or applications.

STOP ADVANCED THREATS

Detects targeted and advanced attacks without requiring any prior knowledge of the threat form, type, or behavior.

The platform detects known and unknown threats at the earliest stage of an attack lifecycle.



CUT OPERATIONAL COSTS

Does not collect tons of data, not generate false positive alerts, no need for special skills to operate.

It deploys easily into existing security infrastructures and does not generate false positives.

AUTOMATED INCIDENT RESPONSE

Accelerates IR through 3rd party integrations that automate isolation, blocking, and threat hunting.

MINIMUM MANUAL CONFIGURATION

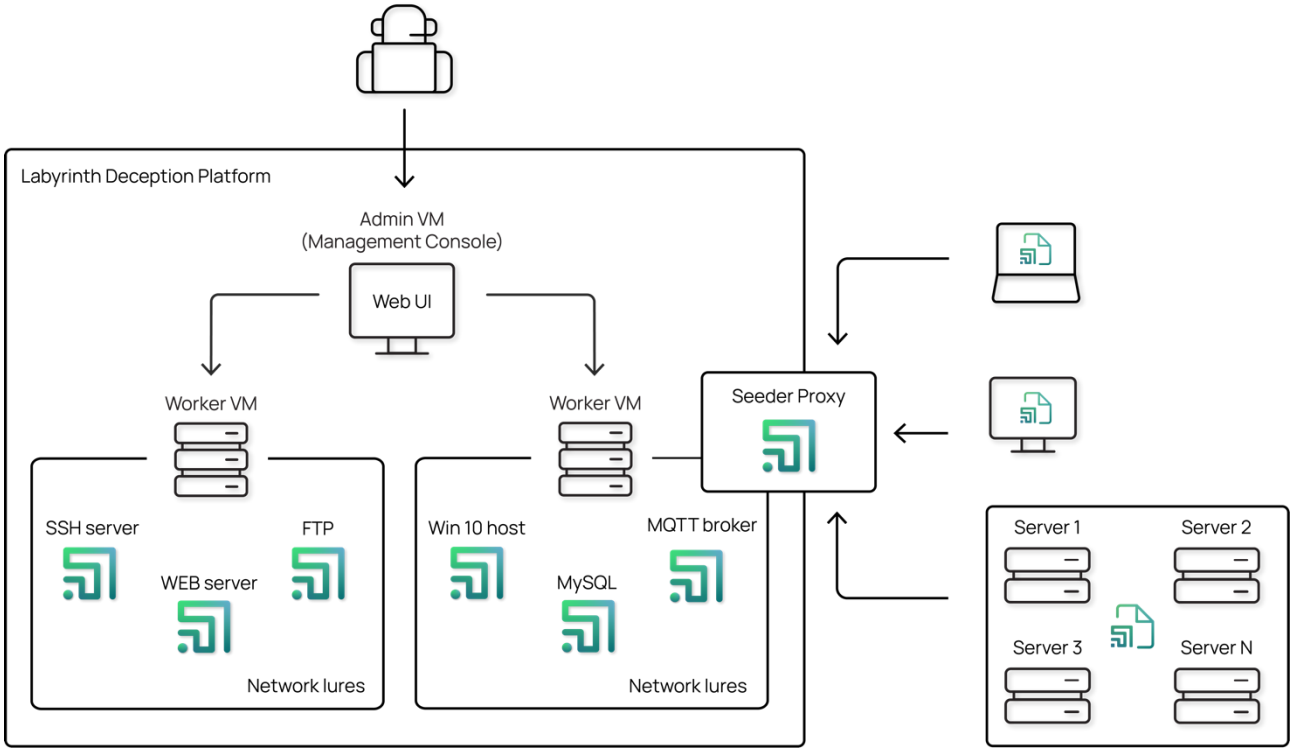
Fast and simple rollout with no system conflicts and minimum maintenance: no databases, signatures, or rules to configure and update.

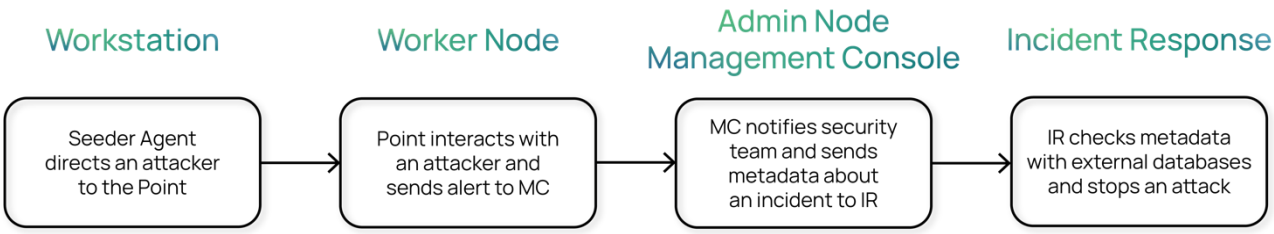
ARCHITECTURE

The Labyrinth Platform automatically deploys Honeynets based on the information about network environment and devices in use. Also, decoys can be deployed manually via the Management Console.

It gives companies a powerful tool to develop their own unique Deception Platform based on their special needs and global best practices.

The Platform provides adversaries with an illusion of IT services and applications vulnerabilities, provokes them for actions, detects and monitors all their activities, and isolates them from real IT network.





KEY FEATURES

Labyrinth Deception Platform does not emulate actual IT infrastructure. Instead, the Platform provides attackers with an illusion of real IT network vulnerabilities. The Labyrinth Technology Team continuously updates the solution with imitations of newly discovered vulnerabilities. It makes Labyrinth a very efficient tool for Advanced Threats detection and response.

HIGH INTERACTION HONEYPOTS

Labyrinth Deception Platform is based on Points – high interaction honeypots with intelligent features. Points are identical to the enterprise assets and run real operating systems, applications and services with fake data.

They allow an attacker to log in and respond to the attacker's request to understand their intentions. Points lure them for a long time, observing them and collecting valuable data about their tools and technics. Besides that, Points produce local Indicators of Compromise (IoCs) and machine-readable threat intelligence (MRTI).

POINTS VARIETY AND AUTHENTICITY

Labyrinth Points reflect production network vulnerabilities, emulating real OS/image, services, and applications for IoT, SCADA/OT, POS, ICS, network and telecommunications environments. False workstations, servers, devices, applications, services, and protocols look identical to real assets.

Labyrinth Points not only emulate the most attractive for attacker vulnerabilities but also behave as real hosts. Depending on the type, they can send broadcast requests, change IP addresses and connect to news websites. It makes possible to blend decoys in a production environment and stand them out from the rest of the assets, for being chosen as a target for an attacker.

MULTI-LAYER SECURITY

Labyrinth implements a full stack of deception in order to provide the highest level of security for its customers. Low interaction artifacts on the first line of defense are emulating enterprise application and used only for basic threat detection.

They are easy to discover and bypass and tell attackers that they are in a minefield. It turns away opportunistic attackers and gives targeted attackers false confidence that they have discovered deceptions in a network. Meantime, high interaction decoys remain unnoticed and ensure the detection of advanced threats.

CUSTOMIZATION

The Labyrinth Deception Team provides advanced services to develop Labyrinth in complex environments or for special industry needs such as IoT, SCADA or POS. Our cybersecurity specialists are constantly working on finding/revealing new threats. After analysis we develop new Labyrinth Paths and Points to deceive the threat's activity.

Each Labyrinth installation regularly updates its Map with new Paths and Points to provide the best threat deception capabilities. To strengthen defense when an attack is underway, additional Points can be added or Points' types can be changed.

AUTOMATION

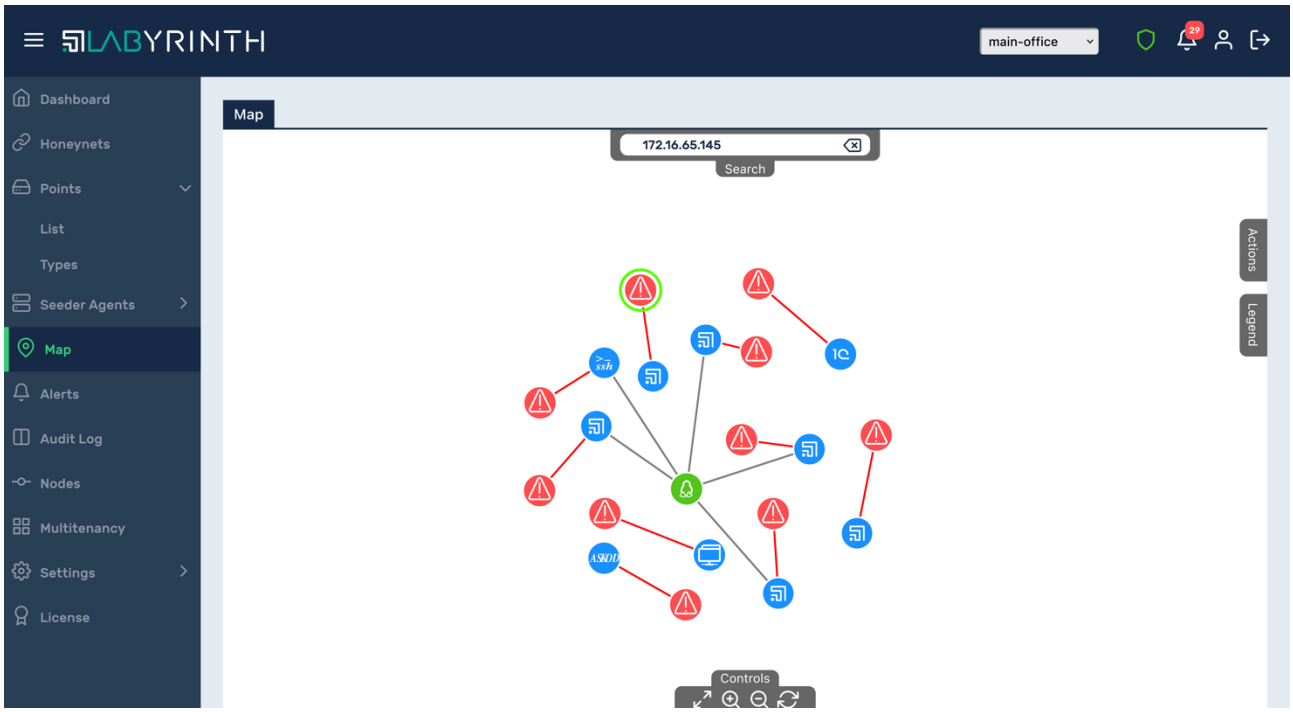
Labyrinth Deception Platform automatically identifies hosts, services and connection paths between them to streamline and adapt the creation and deployment of decoys and honeypots.

The advanced networking features provide capabilities to dynamically build new paths in Labyrinth and to upgrade Points. Labyrinth provides automate management and periodical refresh of deployed in production environment Points to maintain authenticity. The lightweight, automated and flexible solution saves time and provides a high level of security since day one of the deployment.

SCALABILITY

Labyrinth can be efficiently scaled in large distributed enterprise networks. Every emulated Point is a lightweight process that runs on a virtual machine. Thus, Labyrinth scalability does not rely on processing resources, but based on constructing and implementing a coprehensive and realistic set of decoys and honeypots throughout network environment.

Automatic Points creation and deployment helps companies streamline a scaling process and achieve full protection of all network segments.



Labyrinth Deception Platform provides the most efficient tool to detect and stop hackers' movements inside the corporate network.

For more information about Labyrinth of for the product demonstration, please contact us at **info@labyrinth.tech**