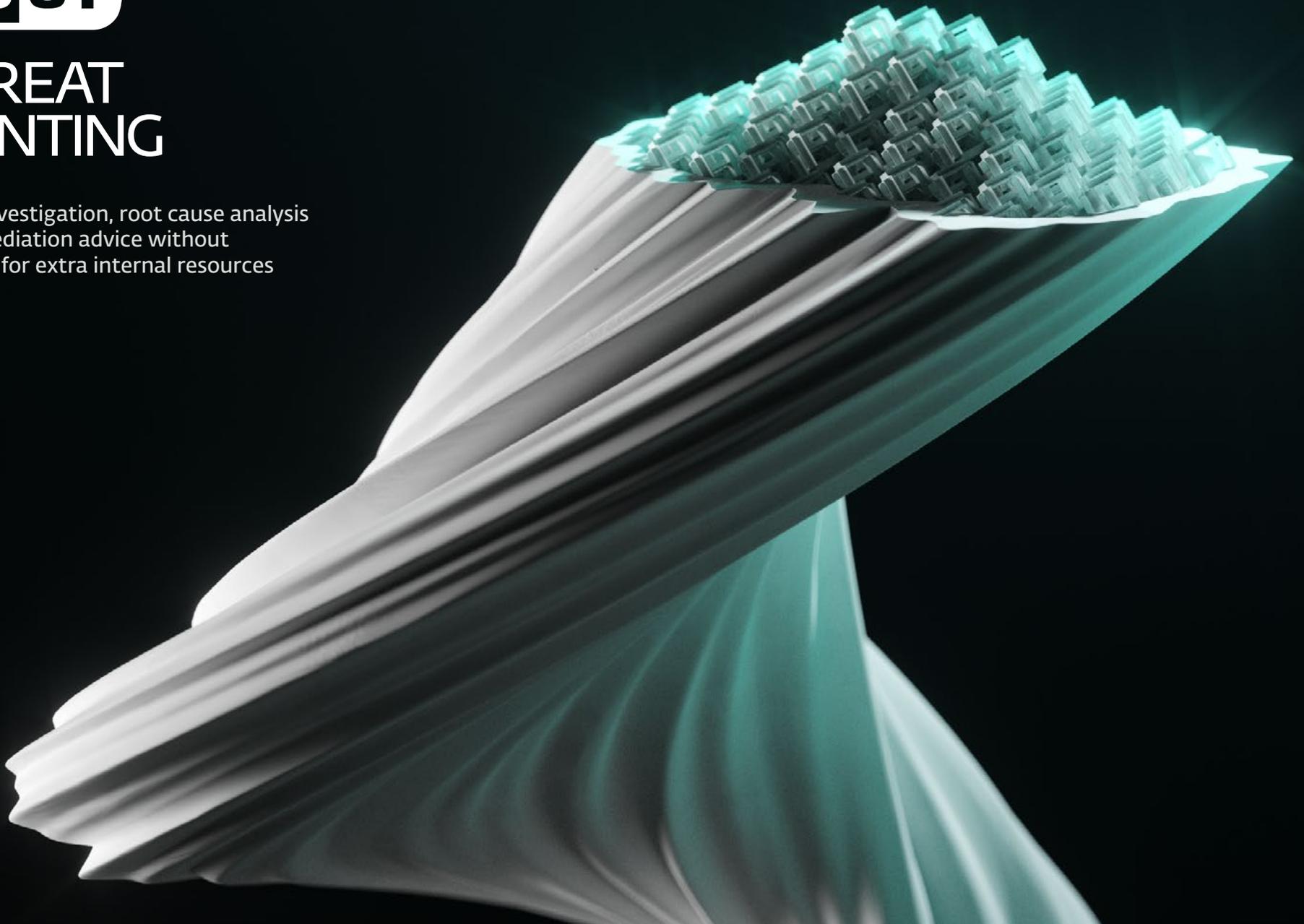


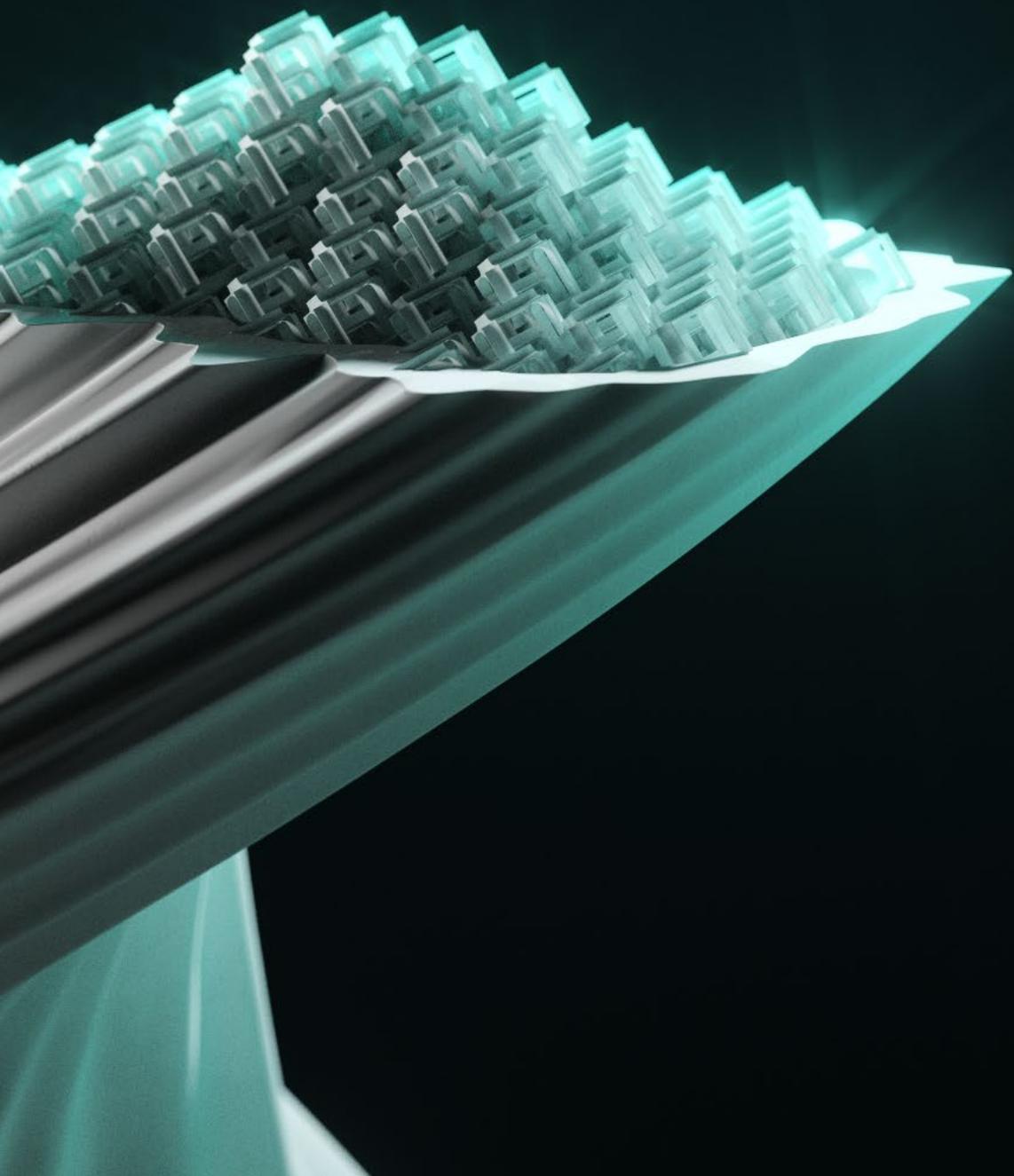


# THREAT HUNTING

Threat investigation, root cause analysis  
and remediation advice without  
the need for extra internal resources







# What is our Threat Hunting service?

ESET Threat Hunting helps your IT teams investigate specific sets of data, events and alarms generated by ESET's endpoint detection and response (EDR) solution—ESET Enterprise Inspector.

This allows you to conduct full forensic investigations without the need for dedicated staff or resources.

# The challenges



## LACK OF PRODUCT KNOWLEDGE

Utilizing new products without previous experience of them can be tricky even for organizations with dedicated security or IT teams. In addition, keeping up with the rapidly changing cyber threat landscape can be challenging and is sometimes best left to experts.



## LONG-TERM COSTS

Creating dedicated teams and/or hiring specialists to perform niche occasional tasks can incur high long-term costs. Purchasing products and services from a single vendor provides accounting departments peace of mind, especially for multinational corporations.



## LACK OF MANPOWER

Security teams and IT administrators need to prioritize their workload by pinpointing only important events. In addition, it can take months to hire and train a team to implement and monitor an endpoint detection and response platform.

# Why ESET Threat Hunting service?



Keeping up with the rapidly changing cyber threat landscape can be challenging, and is sometimes best left to experts.



It can take months to hire and train a team to implement and monitor endpoint detection and response technology.



## GET THE MOST OUT OF ESET'S EDR

ESET Enterprise Inspector is a sophisticated EDR tool for identification of anomalous behavior and breaches, risk assessment, incident response, investigation and remediation. It monitors and evaluates all activities happening in the network in real time and allows organizations to take immediate action if needed.

ESET Enterprise Inspector is a prerequisite for ESET Threat Hunting service

# ESET Threat Hunting: Technical features

## **ON-DEMAND**

Your IT teams can contact ESET Threat Hunting operators when they require Threat Hunting services.

## **ROOT CAUSE ANALYSIS**

Threat Hunting operators review highlighted alarms to determine their root cause.

## **ACTIONABLE ADVICE**

Operators review alarms and compile their findings into a comprehensible status report that includes actionable advice for your organization.

## **SUBSCRIPTION-BASED**

Organizations purchase Threat Hunting services in customizable time blocks during which ESET experts are ready to investigate threats when most needed.

## **ON-PREMISE DATA**

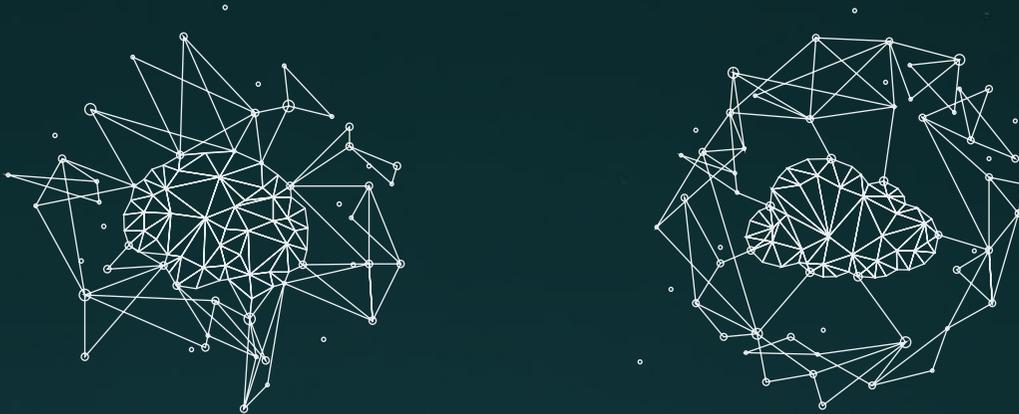
All threat and customer data continue to stay on-premise thanks to a secure remote connection established via the built-in functionality in ESET EDR.

## **INITIAL ASSESSMENT**

A thorough initial assessment is completed to assess your organizations security policies as well as develop an internal profile.

# The ESET difference

Human expertise backed by machine learning. Our reputation system, LiveGrid® is made up of 110 million sensors worldwide, and verified by our R&D centers.



# The stages

## INITIAL ASSESSMENT

- ◆ Each service starts with an assessment of not just your environment, but your organizational composition and general cyber security posture.
- ◆ A full interview is completed with relevant staff members to collect all required information.
- ◆ The result of this phase is an Organization Security Profile, which can be consulted in the future by any Threat Monitoring operator that requires specifics related to your organization, in order to make correct judgments.
- ◆ Your organization is then recommended to contact ESET with any changes to its environment due to the on-demand nature of the Threat Hunting service.

## REGULAR OPERATION

- ◆ When requested, ESET Security experts begin the investigation of pinpointed events to determine their root cause and provide actionable advice.
- ◆ Findings from each investigation are compiled into comprehensible status reports that express technical details in human-readable language.

# Recommended services and solutions

## ESET Detection and Response Ultimate

Combining the skills of our world-class IT security research teams and the cutting-edge technology of our IT security products.

---

## ESET PROTECT Enterprise

Cyber risk management and visibility into your IT environment. Stay one step ahead of any known or unknown threats.

“

*The implementation was very straightforward. In cooperation with ESET's well-trained technical staff, we were up and running our new ESET security solution in a few hours.*

”

IT Manager; Diamantis Masoutis S.A.,  
Greece; 6.000+ seats

“

*We were most impressed with the support and assistance we received. In addition to being a great product, the excellent care and support we got was what really led us to move all of Primoris' systems to ESET as a whole.*

”

Joshua Collins, Data Center Operations Manager; Primoris Services Corporation, USA; 4.000+ seats

# About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services, delivering instant, comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide. ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.

## ESET IN NUMBERS

**110 m+**  
users  
worldwide

**400 k+**  
business  
customers

**200+**  
countries &  
territories

**13**  
global R&D  
centers

## SOME OF OUR CUSTOMERS



protected by ESET since 2016  
more than 14.000 endpoints



ISP security partner since 2008  
2 million customer base



protected by ESET since 2017  
more than 14,000 endpoints



**Allianz**   
Suisse

protected by ESET since 2016  
more than 4,000 mailboxes

# Why choose ESET?

## SOME OF OUR TOP AWARDS



## ISO SECURITY CERTIFIED



### ISO SECURITY CERTIFIED

ESET is compliant with ISO/IEC 27001:2013, an internationally recognized and applicable security standard in implementing and managing information security. The certification is granted by the third-party accredited certification body SGS and demonstrates ESET's full compliance with industry-leading best practices.

## ANALYST RECOGNITION

### FORRESTER®

ESET was included in the Now Tech: Enterprise Detection And Response, Q1 2020 report — Forrester's overview of 29 enterprise Detection and Response solutions.



ESET retains its 'Top Player' status in Radicati's 2021 APT Protection Market Quadrant report.

Gartner Peer Insights is a free peer review and ratings platform designed for enterprise software and services decision makers. Reviews go through a strict validation and moderation process to ensure information is authentic. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences, and do not represent the views of Gartner or its affiliates.

