ENJOY SAFER TECHNOLOGY™

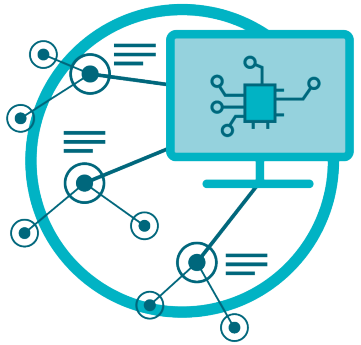
ESET Teknolojileri

Can Erginkurban
Product & Marketing Manager

ESET teknolojilerinin dört ayağı

Koruma Katmanları

ESET LiveGrid®



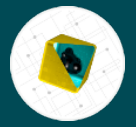
Makine Öğrenimi

İnsan Deneyimi

UEFI Scanner

Network Attack Protection

Reputation & Cache



In-product Sandbox

Exploit Blocker

Ransomware Shield

DNA Detections

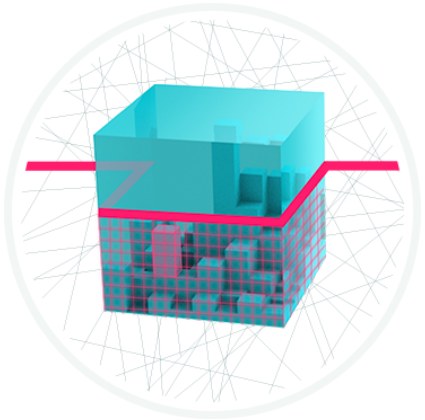
LiveGrid® Protection

Botnet Protection

Advanced Memory Scanner

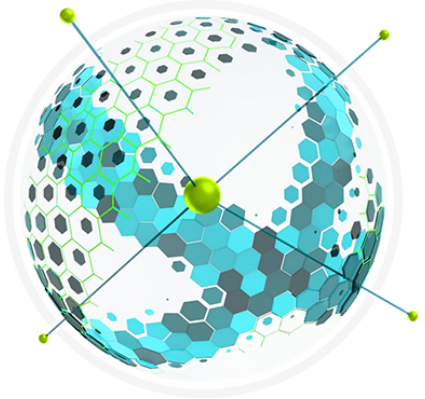
Script Scanner (AMSI)

- PRE EXECUTION
- EXECUTION
- POST EXECUTION



Unified Extensible Firmware Interface (UEFI) Scanner

ESET önyükleme ortamını kontrol ederek güvenliğini sağlamakla görevli bir katmanı ürünlerine ekleyen ilk üretici.



Network Attack Protection

Ağ iletişimini denetler, tespit eder ve engeller

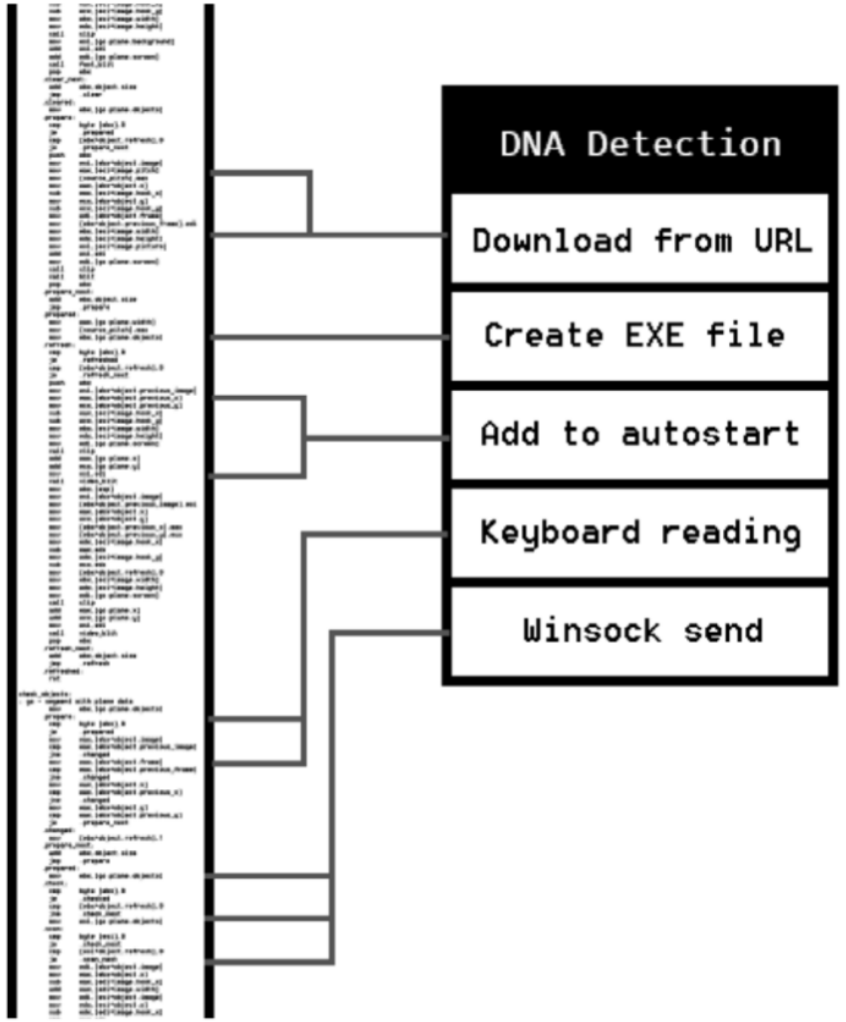
- **Büyük botnetler**: Bayrob, Bedep, Boaxxe
- **Truva atı indirenler**: Adload, Banload, Dagozil, Wauchos, Upatre, Zurgop
- **Casus Yazılımlar**: Zbot, Banker, Agent.(çeşitleri)
- **Dosya Şifreleyiciler**: Cryptowall
- **İstismar Kitleri**: Sundown, Neutrino, Magnitude, Stegano EK, Rig, MWI
- **Diğer web tehditleri**: RouterDNSChanger, Mailspam

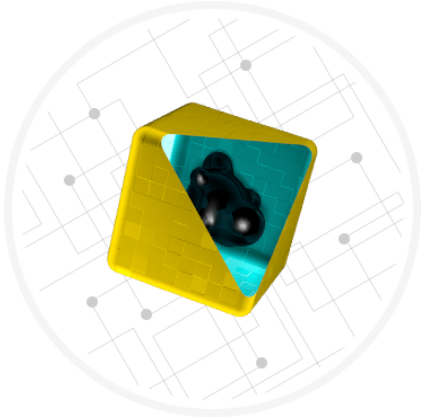
Reputation & Cache

- Dosya veya URL gibi bir nesneyi incelerken, taramadan önce ürünlerimiz yerel önbelleği kontrol ederek bulaşıcı veya zararlı nesneler olmadığından emin olur.
- Nesneler **LiveGrid İtibar** sisteminde sorgulanır. Bu da tarama etkinliğini arttırarak zararlı yazılım bilgilerinin müşterilerimiz arasında hızla yayılmasını sağlar.
- URL kara listeleri ve itibar sistemi, kullanıcıların zararlı içerikli sitelere veya phishing sitelerine erişmelerini engeller.

DNA detections

- Özelliklerin yüksek düzeyde gösterimi
  - Statik analiz (deobfuscation)
  - Dinamik analiz (emulation)
- Tüm potansiyel zararlı dosya türleri için DNA tespiti





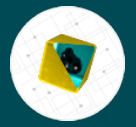
In-product Sandbox

- Karmaşık polimorfik zararlıları emule ederek açık formlarını ortaya çıkarır.
- Milisaniyeler içinde çalışır, hafif ve etkilidir.
- Platform bağımsızdır.

UEFI Scanner

Network Attack Protection

Reputation & Cache



In-product Sandbox

Exploit Blocker

Ransomware Shield

DNA Detections

LiveGrid® Protection

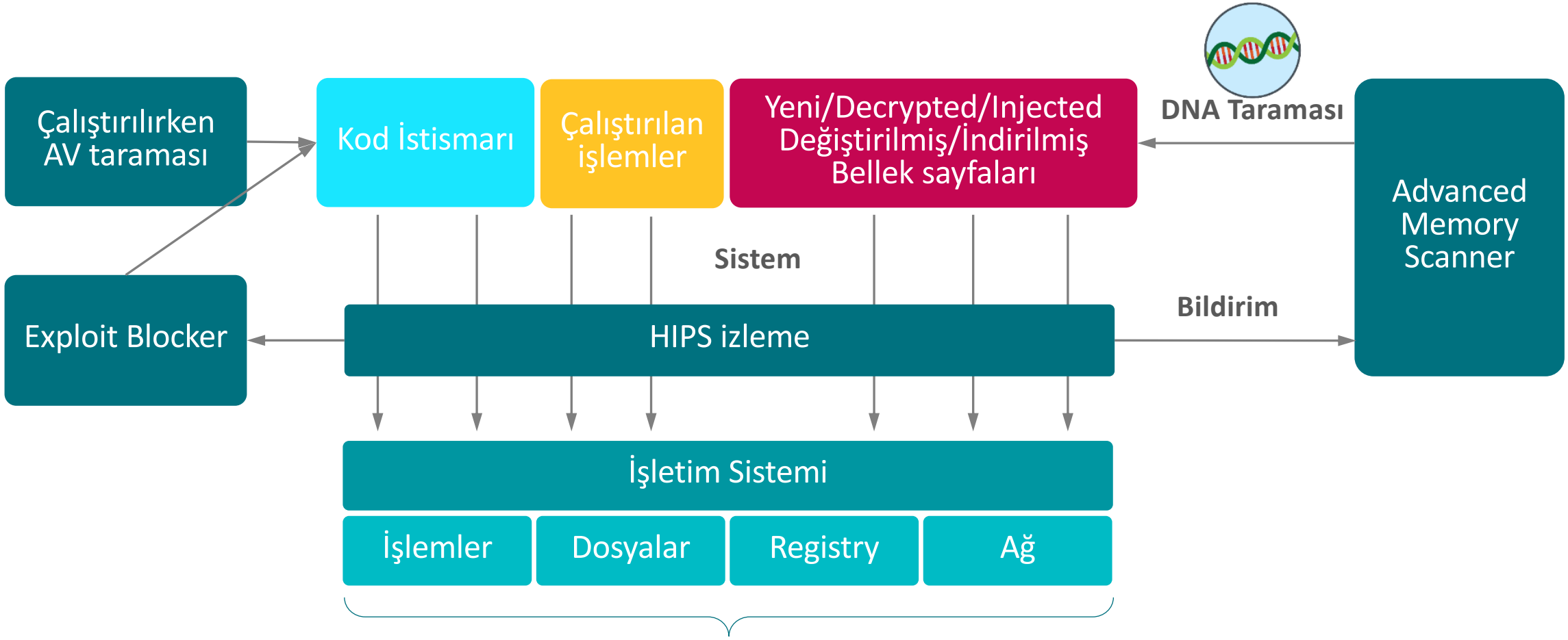
Botnet Protection

Advanced Memory Scanner

Script Scanner (AMSI)

- PRE EXECUTION
- EXECUTION
- POST EXECUTION

Advanced Memory Scanner



Davranışsal paternler tespit edilir ve engellenir
Kurallar uygulanır

Exploit Blocker

Sıkça hedeflenen ve açık veren uygulamaları izler.

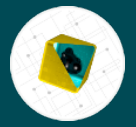
Ransomware Shield

- Ransomware başka bir malware türüdür.
- 110 milyon sensör ve anonim LiveGrid verileri yeni ransomware saldırılarını bildirir.
- Davranışsal (jenerik, aileye özel, dosya tabanlı) ve itibar tabanlı sezgisel tespit.

UEFI Scanner

Network Attack Protection

Reputation & Cache



In-product Sandbox

Exploit Blocker

Ransomware Shield

DNA Detections

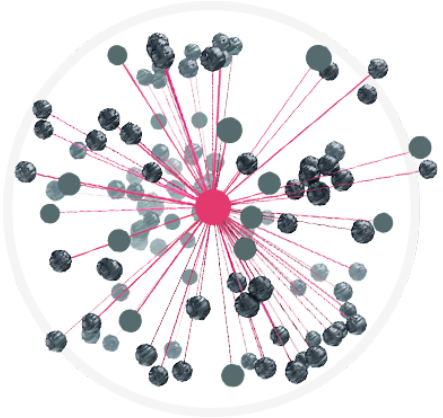
LiveGrid® Protection

Botnet Protection

Advanced Memory Scanner

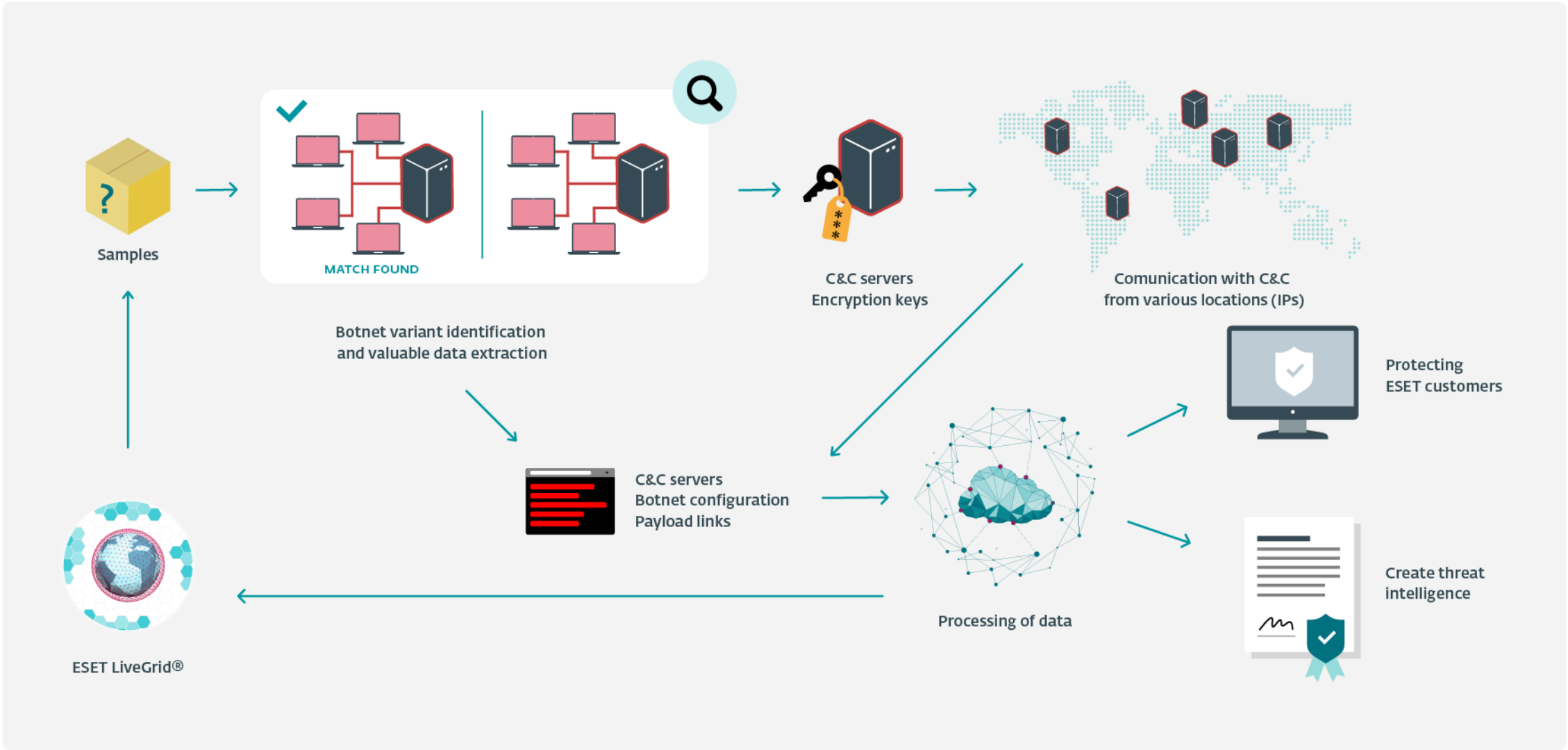
Script Scanner (AMSI)

- PRE EXECUTION
- EXECUTION
- POST EXECUTION



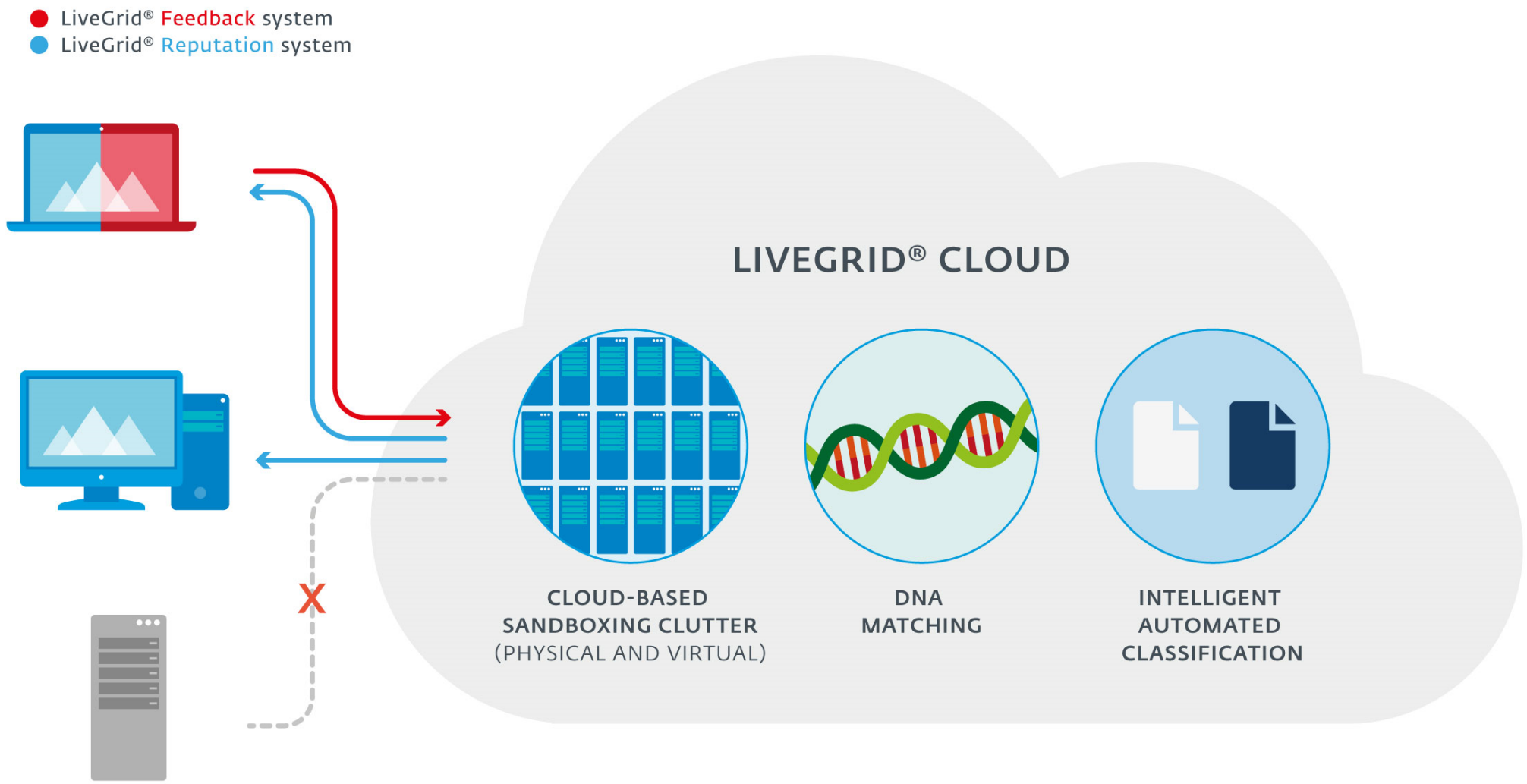
Botnet Protection

Çalıştırılmadan önce | Çalıştırılırken | **Çalıştırıldıktan sonra** | Sürekli

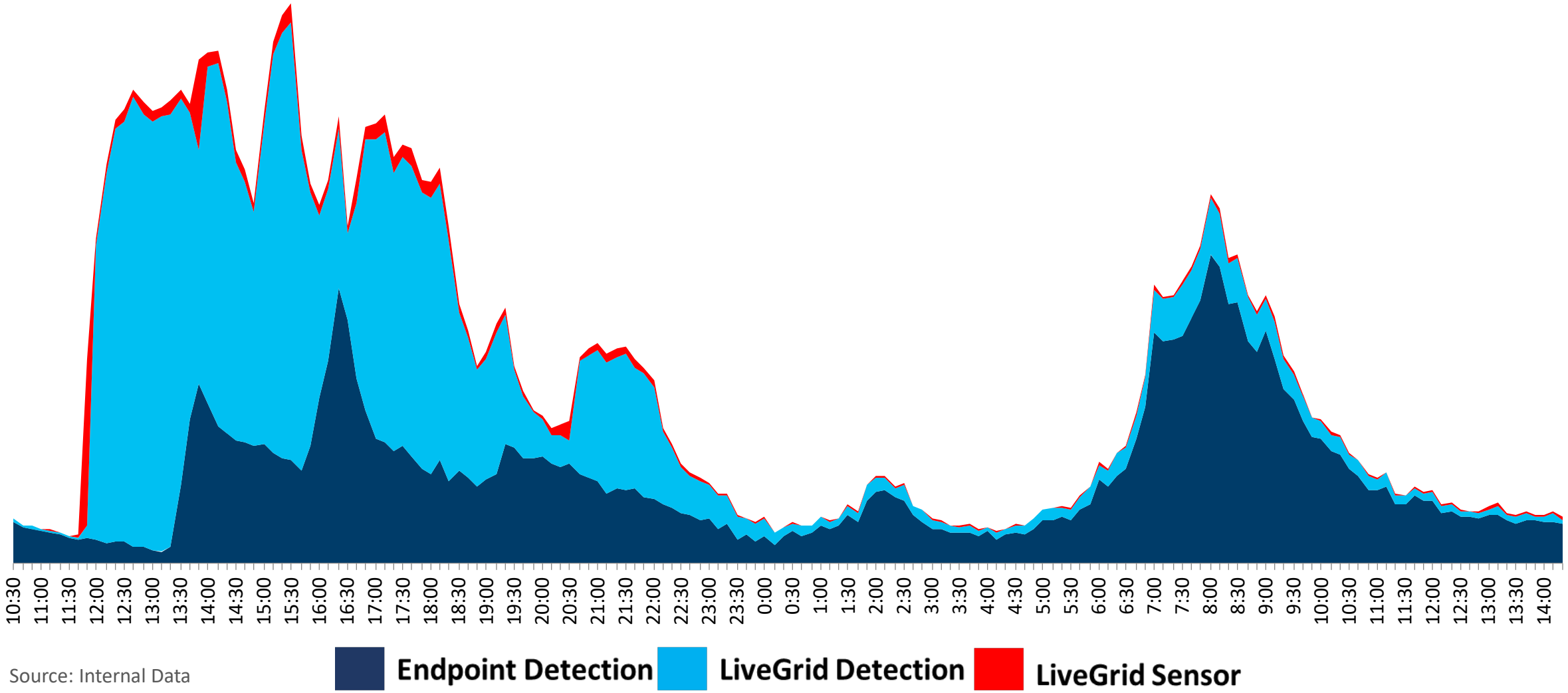


ESET LiveGrid®

110+ milyon cihaz, verileri ESET LiveGrid®'e raporluyor.

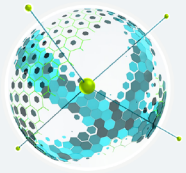

LiveGrid® Feedback system
LiveGrid® Reputation system
LIVEGRID® CLOUD
CLOUD-BASED SANDBOXING CLUTTER (PHYSICAL AND VIRTUAL)
DNA MATCHING
INTELLIGENT AUTOMATED CLASSIFICATION

ESET LiveGrid® Daha Hızlı Tepki Demek

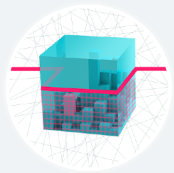


Source: Internal Data

Endpoint detection & data collection & labeling

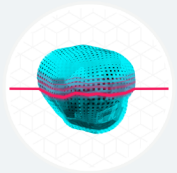


Network Attack Protection

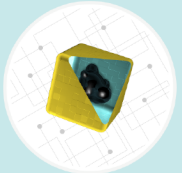


UEFI Scanner

Code analysis & scanning / Features extraction / Machine Learning based detection



Advanced Memory Scanner



In-product Sandbox

DNA Detection

Ransomware Shield

Exploit Blocker

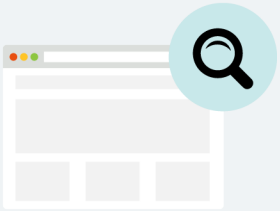
Botnet Protection

ESET LiveGrid®

Machine learning phase

Machine learning phase analysis

Machine learning model generation

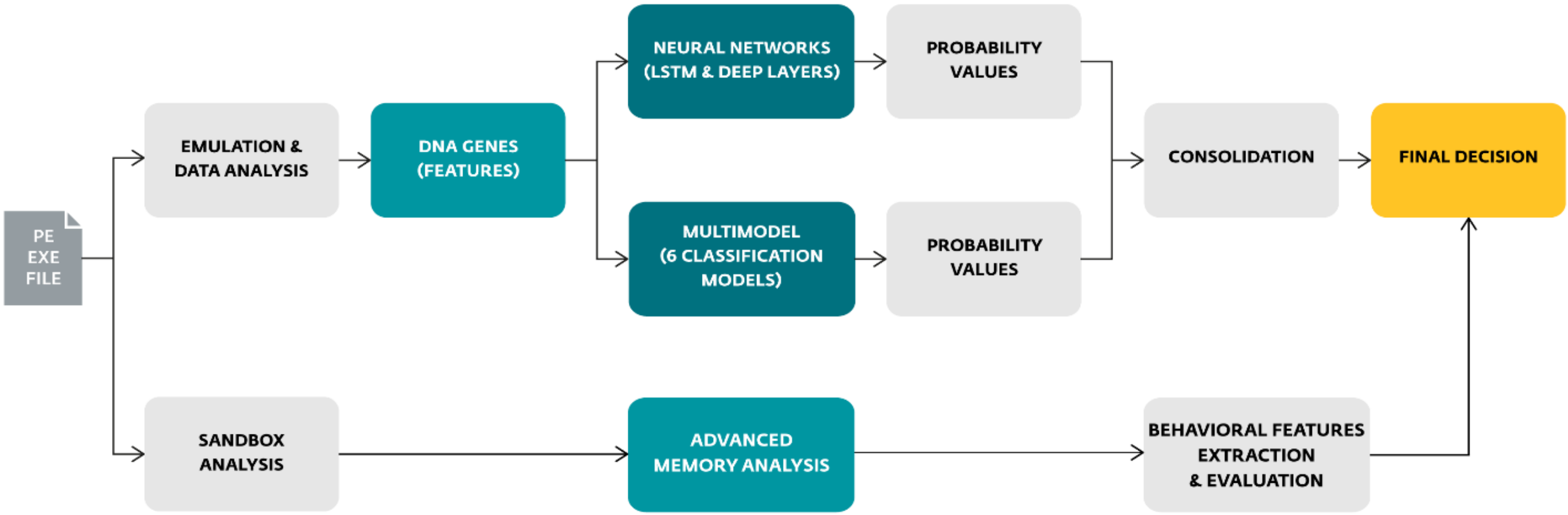


URLs

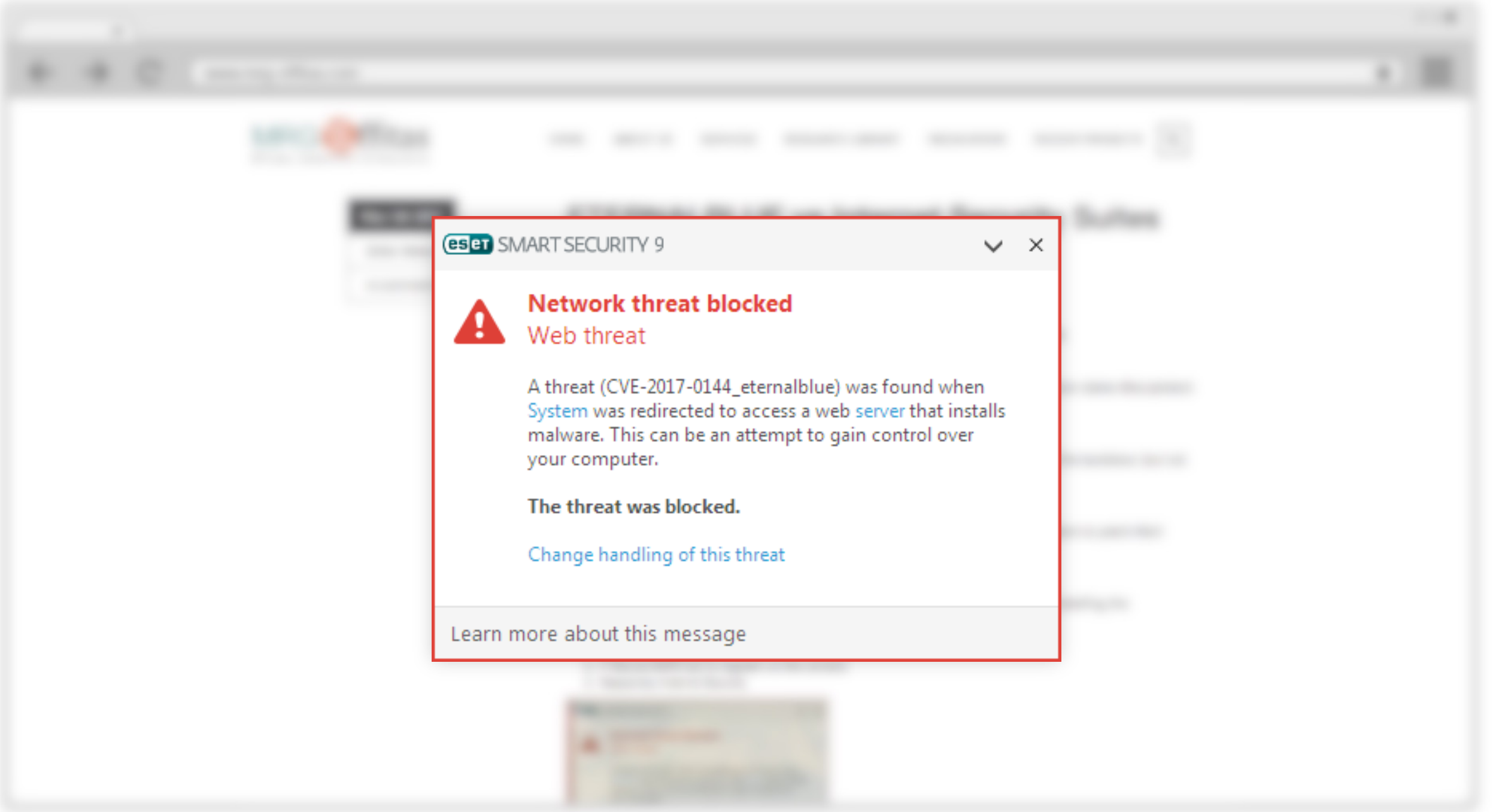
Binaries

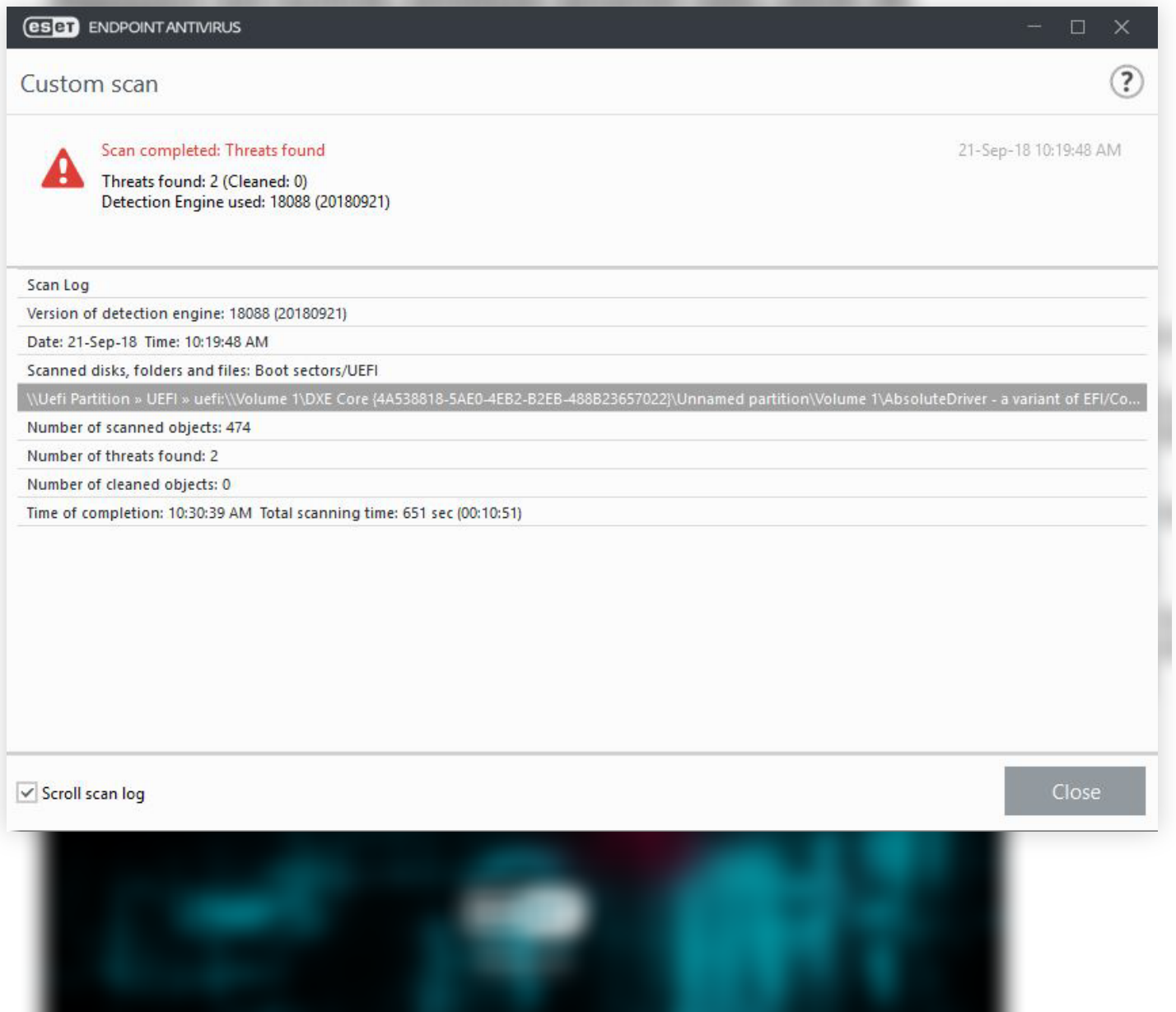
UPDATE

ESET Machine Learning akışı




Gerçek örnekler


ESET SMART SECURITY 9
Network threat blocked
Web threat
A threat (CVE-2017-0144_eternalblue) was found when System was redirected to access a web server that installs malware. This can be an attempt to gain control over your computer.
The threat was blocked.
Change handling of this threat
Learn more about this message


ENDPOINT ANTIVIRUS
Custom scan
Scan completed: Threats found
21-Sep-18 10:19:48 AM
Threats found: 2 (Cleaned: 0)
Detection Engine used: 18088 (20180921)
Scan Log
Version of detection engine: 18088 (20180921)
Date: 21-Sep-18 Time: 10:19:48 AM
Scanned disks, folders and files: Boot sectors/UEFI
\\Uefi Partition » UEFI » uefi:\\Volume 1\DXE Core {4A538818-5AE0-4EB2-B2EB-488B23657022}\Unnamed partition\Volume 1\AbsoluteDriver - a variant of EFI/Co...
Number of scanned objects: 474
Number of threats found: 2
Number of cleaned objects: 0
Time of completion: 10:30:39 AM Total scanning time: 651 sec (00:10:51)
Scroll scan log
Close

CYBERSECURITY
EXPERTS ON YOUR SIDE

Teşekkürler...

Can Erginkurban
Product & Marketing Manager