Bitdefender®

WWW.BITDEFENDER.COM

AGENDA

Miért a Bitdefender?

GravityZone védelmi rétegek

Sandbox és Risk Analytics

Endpoint Detection and Response (EDR)

Network Traffic Security Analytics (NTSA)

- TÖBB MINT **500 MILLIÓ** VÉDETT VÉGPONT
- A CYBERSECURITY GYÁRTÓK **38%**-A HASZNÁL BITDEFENDER TECHNOLÓGIÁT
- TÖBB MINT **150 OEM** PARTNER VILÁGSZERTE

solarwinds msp OPSWAT. KERIO

FIREEYE™ GFI Software™

RECOGNIZED BY

GLOBAL SECURITY ANALYSTS & REVIEWERS

FORRESTER
WAVE
LEADER 2019
Cloud Workload Security

Leader in the inaugural Forrester® WAVE ™ for Cloud Workload Security

AV comparatives
CERTIFIED
ATP Enterprise
2019

100% detection in the first Advanced Real-World test by AV-Comparatives

BITDEFENDER
GravityZone Ultra v6.6.7.106
ADVANCED ENDPOINT PROTECTION
NSS Labs
RECOMMENDED

"Received a score of 100% for evasions. No false positives" NSS Labs

Bitdefender

TRUSTED BY

ENTERPRISES AND LAW ENFORCEMENT AGENCIES

PROTECTING KEY ORGANIZATIONS WORLDWIDE

Mentor A Siemens Business

TUI

Commerce STATE BANK Earning Relationships

SPEEDWAY MOTORSPORTS, INC.

esurance

YAMAHA

Honeywell

PARTNERING AGAINST CYBER CRIME

FBI

Department of Justice

EUROPOL EUROPEAN LAW ENFORCEMENT AGENCY

RELIED ON

in key technology partnerships

amazon web services Partner Network
TECHNOLOGY PARTNER

CITRIX PARTNER Citrix Ready

NUTANIX READY
INTEGRATED

Microsoft Partner

vmware READY
NETWORKING AND SECURITY

Pivotal
PIVOTAL TECHNOLOGY PARTNER
PREMIER

KIEMELKEDŐ TELSÍTMÉNY

Az elmúlt 7 év mindegyikében kiemelkedő eredményt ért el a független teszteken

AV comparatives ADVANCED+ Real-World Protection DEC 2013
AV comparatives ADVANCED+ Real-World Protection DEC 2014
AV comparatives
AV comparatives Product of the Year 2019
ADVANCED+ Real-World Protection DEC 2016
AV comparatives Product of the Year 2017
AV comparatives Outstanding Security Product 2018

AV TEST
av-test.org
2019
AWARD
BEST PROTECTION
Bitdefender
Endpoint Security (Ultra)

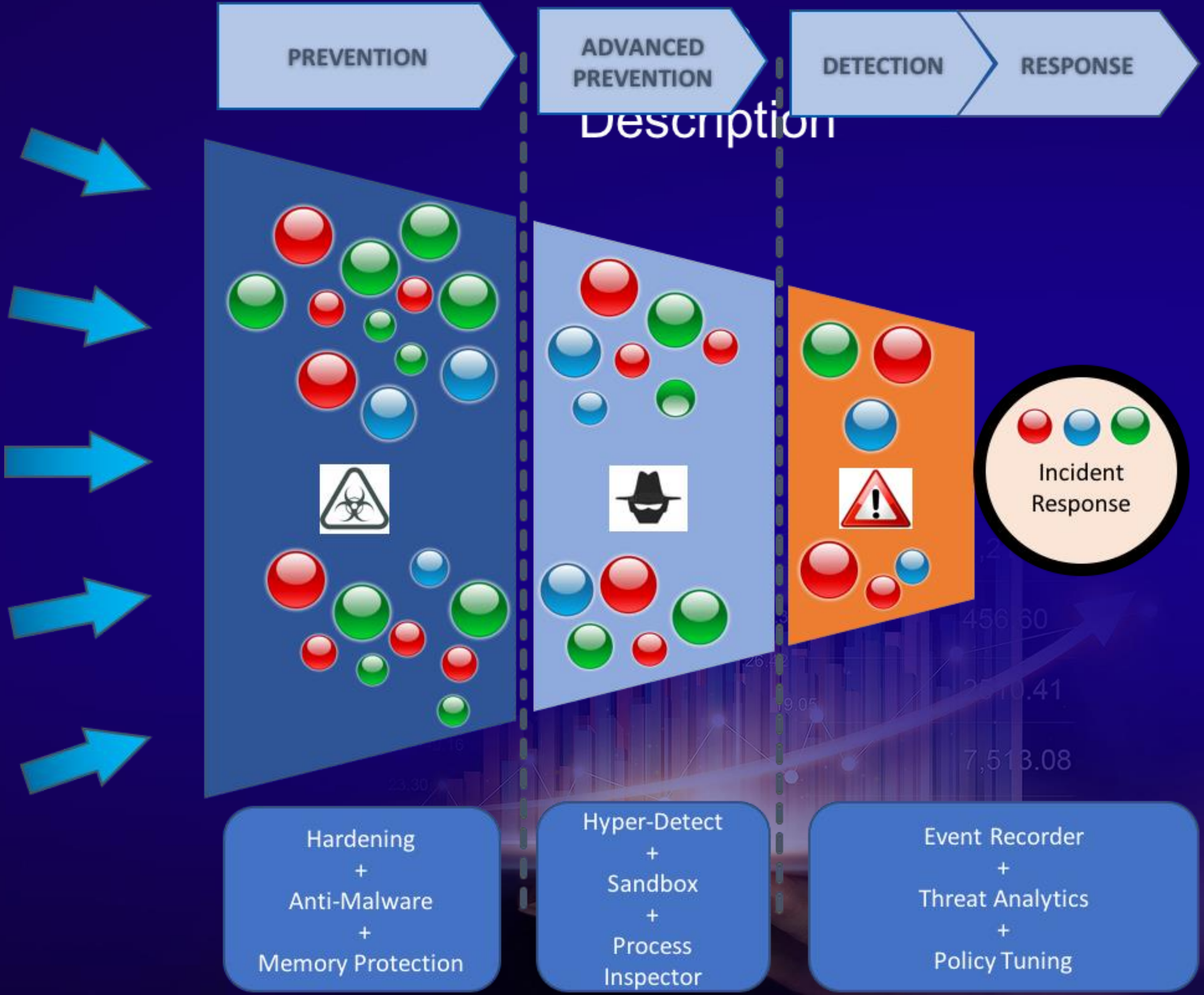
BITDEFENDER
GravityZone Ultra v6.6.7.106
ADVANCED ENDPOINT PROTECTION
NSS LABS
RECOMMENDED
MARCH 2019

FORRESTER®
WAVE
LEADER 2019
Cloud Workload
Security

Risk Management

GravityZone védelmi rétegek:

- Végponti agent
- Risk Analytics
- Sandbox
- EDR
- NTSA



PREVENTION

ADVANCED PREVENTION

DETECTION

RESPONSE

Incident Response

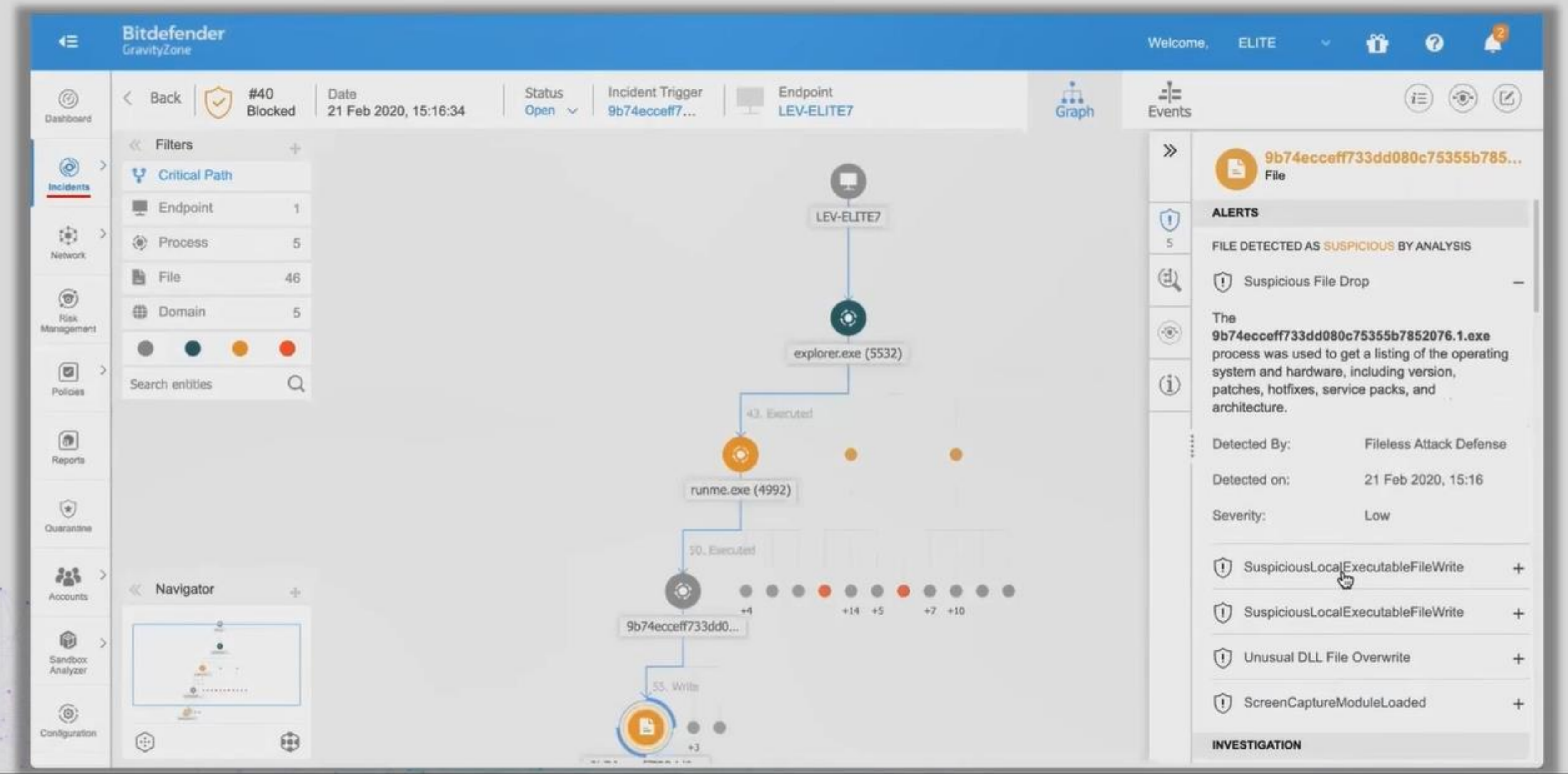
Hardening
+
Anti-Malware
+
Memory Protection

Hyper-Detect
+
Sandbox
+
Process Inspector

Event Recorder
+
Threat Analytics
+
Policy Tuning

Bitdefender

Attack Forensics & Visualizations: The What



#40 Blocked

Date: 21 Feb 2020, 15:16:34

Status: Open

Incident Trigger: 9b74ecceff7...

Endpoint: LEV-ELITE7

Endpoint	1
Process	5
File	46
Domain	5

9b74ecceff733dd080c75355b785...
File

ALERTS

FILE DETECTED AS SUSPICIOUS BY ANALYSIS

Suspicious File Drop

The **9b74ecceff733dd080c75355b7852076.1.exe** process was used to get a listing of the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.

Detected By:	Fileless Attack Defense
Detected on:	21 Feb 2020, 15:16
Severity:	Low

SuspiciousLocalExecutableFileWrite +

SuspiciousLocalExecutableFileWrite +

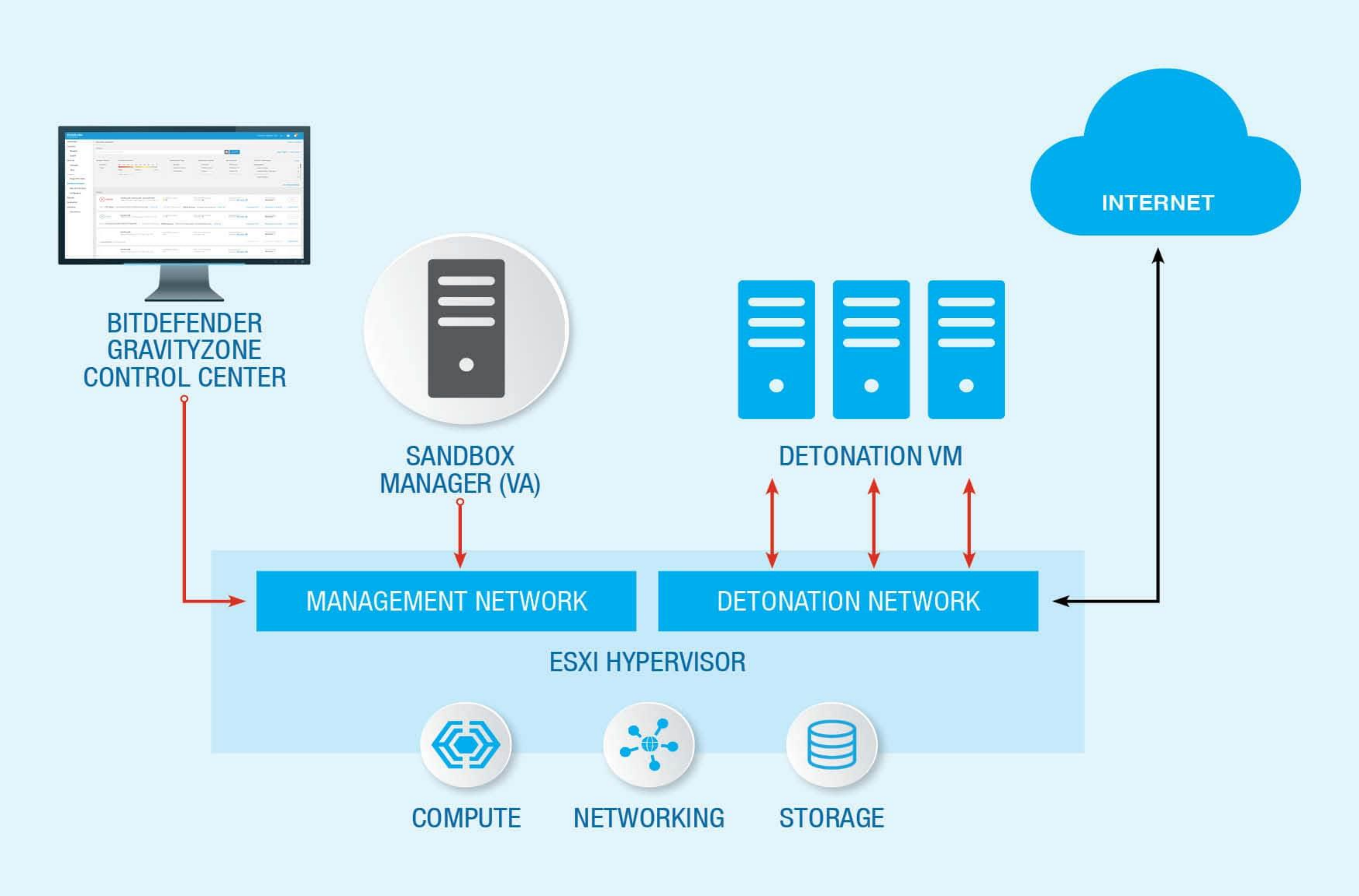
Unusual DLL File Overwrite +

ScreenCaptureModuleLoaded +

INVESTIGATION

Sandbox analyzer

Bitdefender®

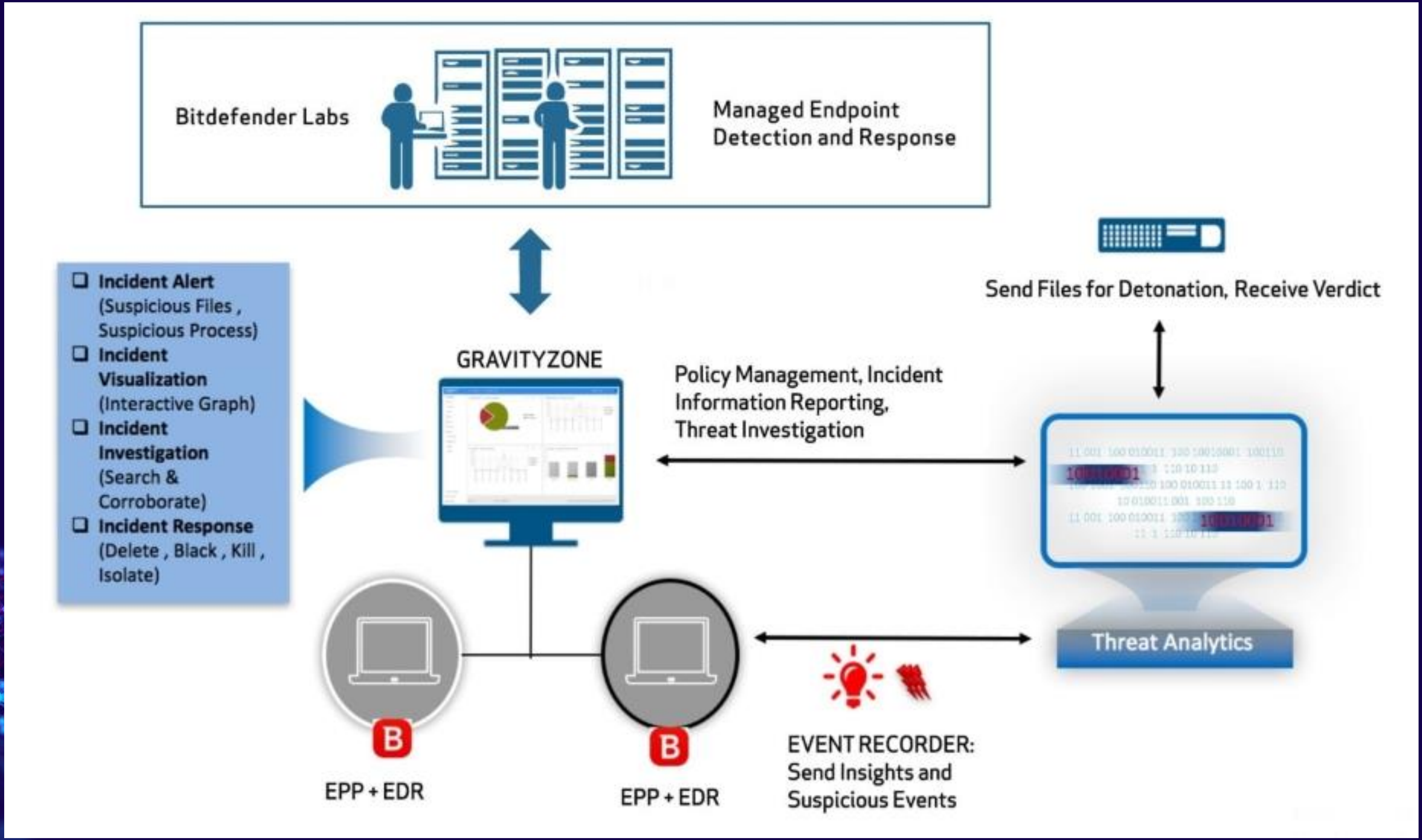


Bitdefender®

GravityZone

Endpoint Detection and Response (EDR/MDR)

Bitdefender®



Bitdefender Labs

Managed Endpoint Detection and Response

- ❑ **Incident Alert** (Suspicious Files , Suspicious Process)
- ❑ **Incident Visualization** (Interactive Graph)
- ❑ **Incident Investigation** (Search & Corroborate)
- ❑ **Incident Response** (Delete , Black , Kill , Isolate)

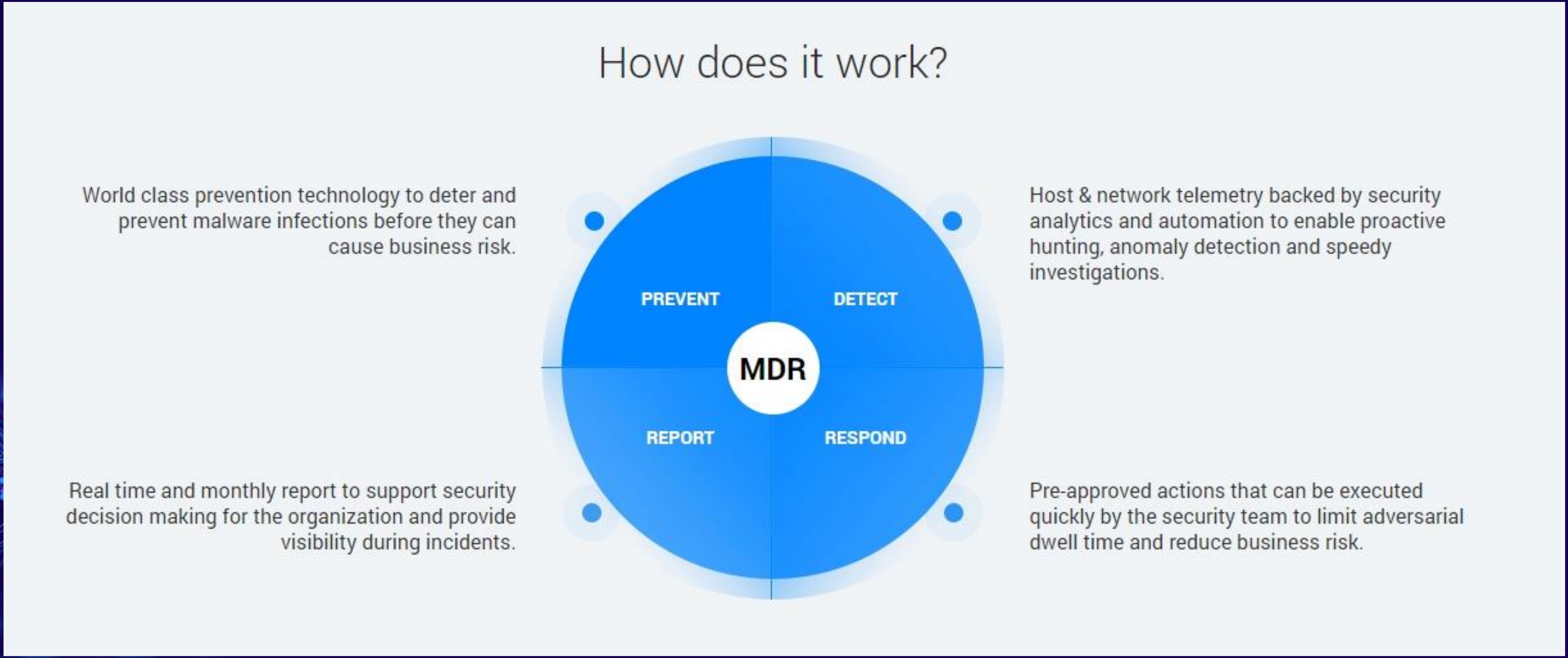
GRAVITYZONE

Policy Management, Incident Information Reporting, Threat Investigation

Send Files for Detonation, Receive Verdict

Threat Analytics

EVENT RECORDER: Send Insights and Suspicious Events



How does it work?

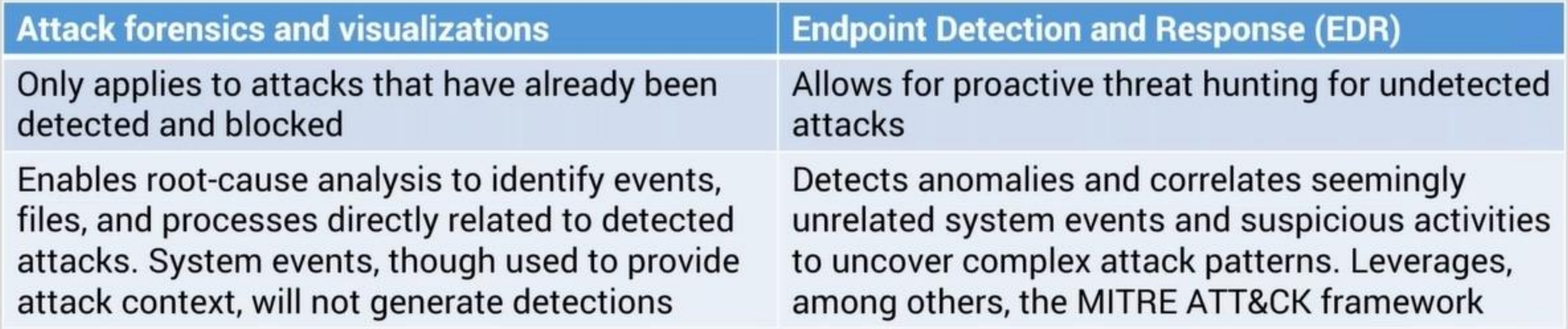
World class prevention technology to deter and prevent malware infections before they can cause business risk.

Host & network telemetry backed by security analytics and automation to enable proactive hunting, anomaly detection and speedy investigations.

Real time and monthly report to support security decision making for the organization and provide visibility during incidents.

Pre-approved actions that can be executed quickly by the security team to limit adversarial dwell time and reduce business risk.

Attack Forensics & Visualizations vs. EDR

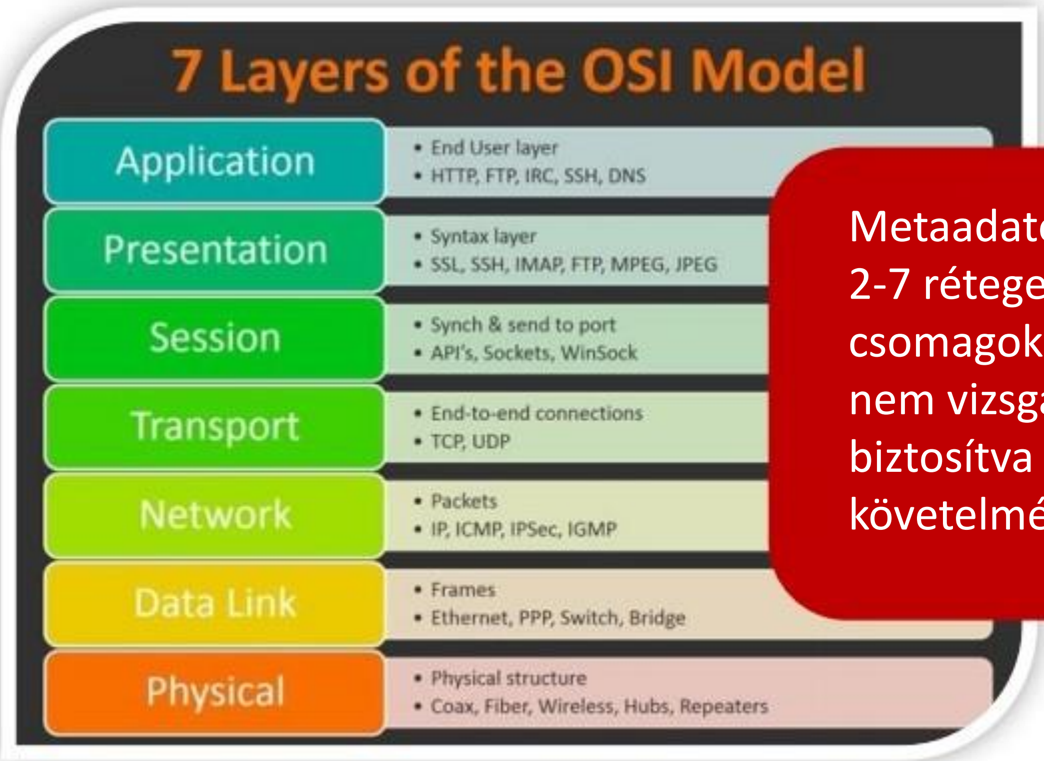


Attack forensics and visualizations	Endpoint Detection and Response (EDR)
Only applies to attacks that have already been detected and blocked	Allows for proactive threat hunting for undetected attacks
Enables root-cause analysis to identify events, files, and processes directly related to detected attacks. System events, though used to provide attack context, will not generate detections	Detects anomalies and correlates seemingly unrelated system events and suspicious activities to uncover complex attack patterns. Leverages, among others, the MITRE ATT&CK framework

Network Traffic Security Analytics (NTSA)

Bitdefender

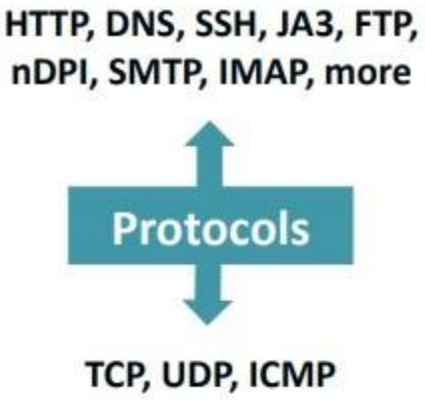
Milyen adatokat vizsgál az NTSA rendszere?

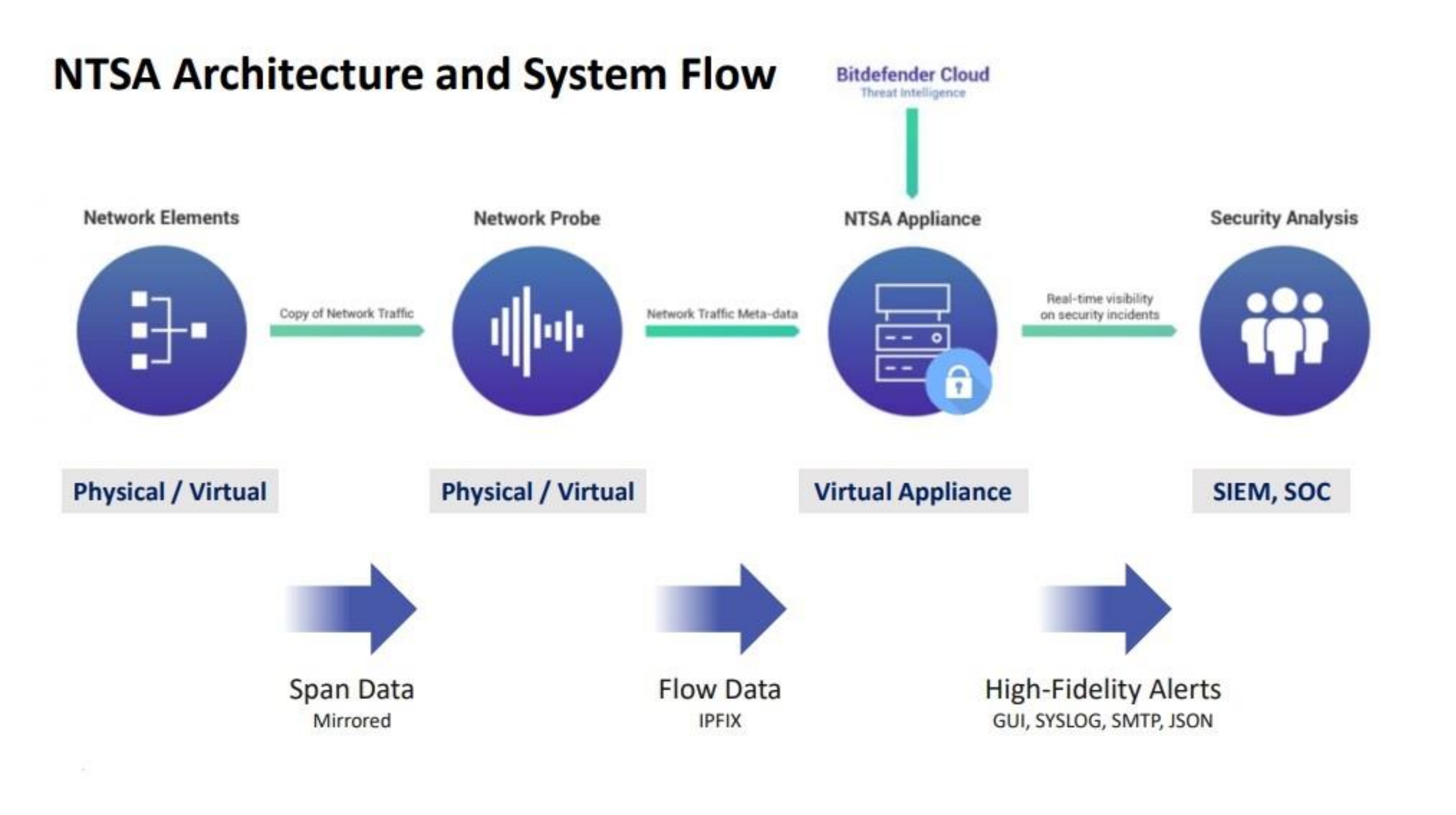


7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

Metaadatok gyűjtése a 2-7 rétegekből, a csomagok tartalmát nem vizsgálja, így biztosítva a GDPR követelményeit





NTSA Architecture and System Flow

Bitdefender Cloud
Threat Intelligence

Network Elements

Copy of Network Traffic

Network Probe

Network Traffic Meta-data

NTSA Appliance

Real-time visibility on security incidents

Security Analysis

Physical / Virtual

Physical / Virtual

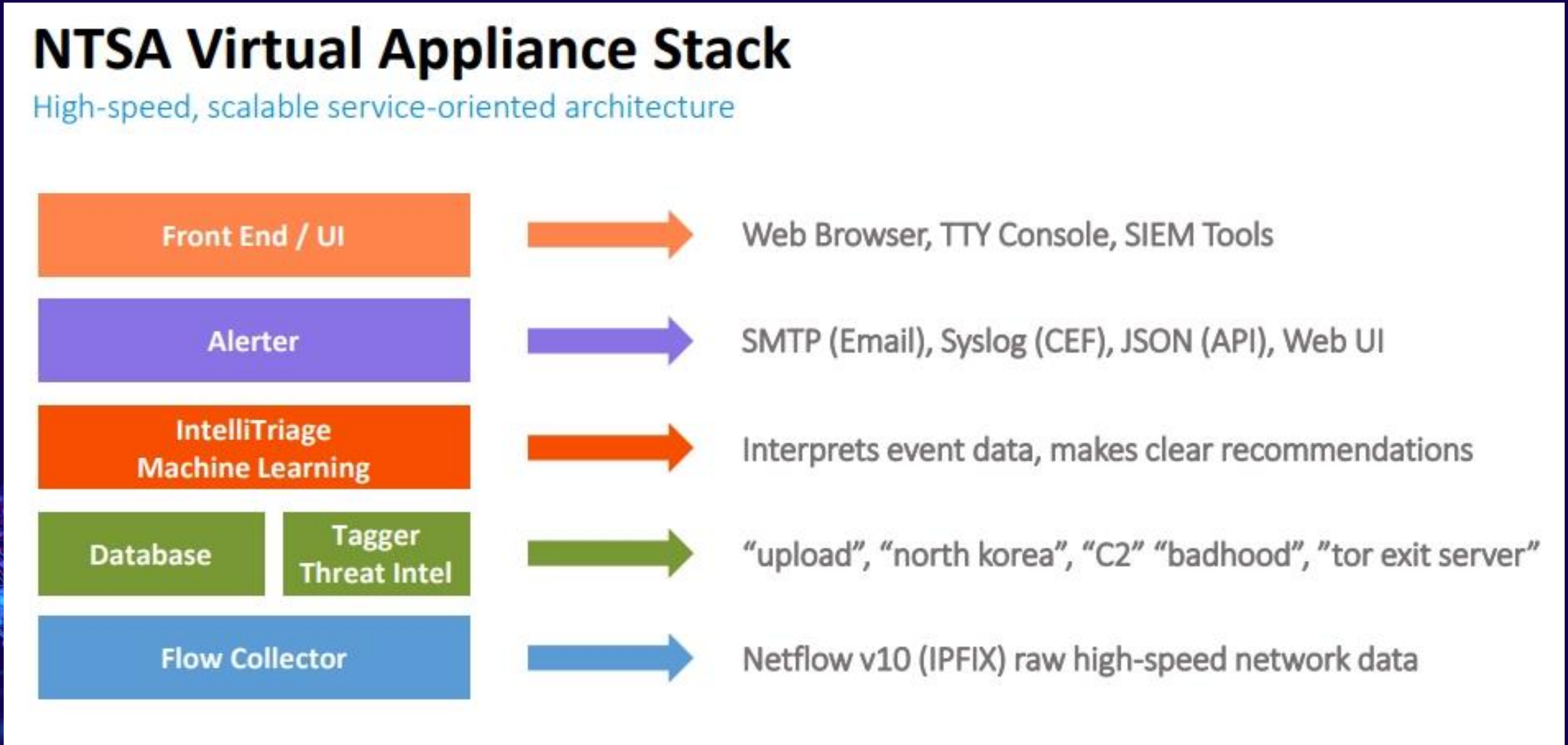
Virtual Appliance

SIEM, SOC

Span Data
Mirrored

Flow Data
IPFIX

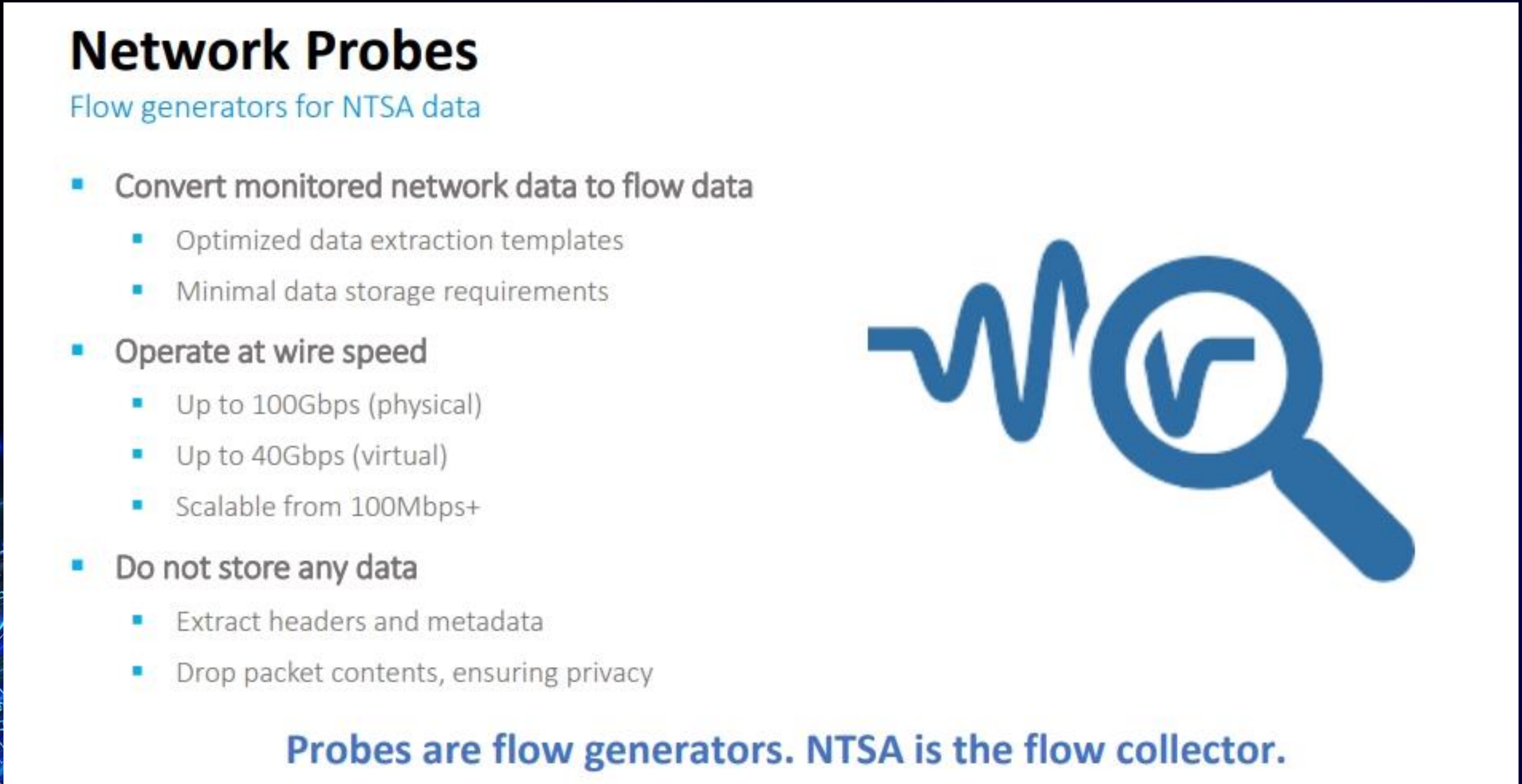
High-Fidelity Alerts
GUI, SYSLOG, SMTP, JSON



NTSA Virtual Appliance Stack

High-speed, scalable service-oriented architecture

Front End / UI	Web Browser, TTY Console, SIEM Tools
Alerter	SMTP (Email), Syslog (CEF), JSON (API), Web UI
IntelliTriage Machine Learning	Interprets event data, makes clear recommendations
Database Tagger Threat Intel	“upload”, “north korea”, “C2” “badhood”, ”tor exit server”
Flow Collector	Netflow v10 (IPFIX) raw high-speed network data



Network Probes

Flow generators for NTSA data

- Convert monitored network data to flow data
  - Optimized data extraction templates
  - Minimal data storage requirements
- Operate at wire speed
  - Up to 100Gbps (physical)
  - Up to 40Gbps (virtual)
  - Scalable from 100Mbps+
- Do not store any data
  - Extract headers and metadata
  - Drop packet contents, ensuring privacy

Probes are flow generators. NTSA is the flow collector.

biztributor

sales@biztributor.hu
+36 1 392-0218
www.biztributor.hu

Bitdefender

Q & A

Bitdefender

WWW.BITDEFENDER.COM