

Bitdefender Network Traffic Security Analytics

REAL-TIME BREACH DETECTION.
AUTOMATED TRIAGE. COMPLETE VISIBILITY

Juan Jesús Merino Torres
National Channel Country Manager

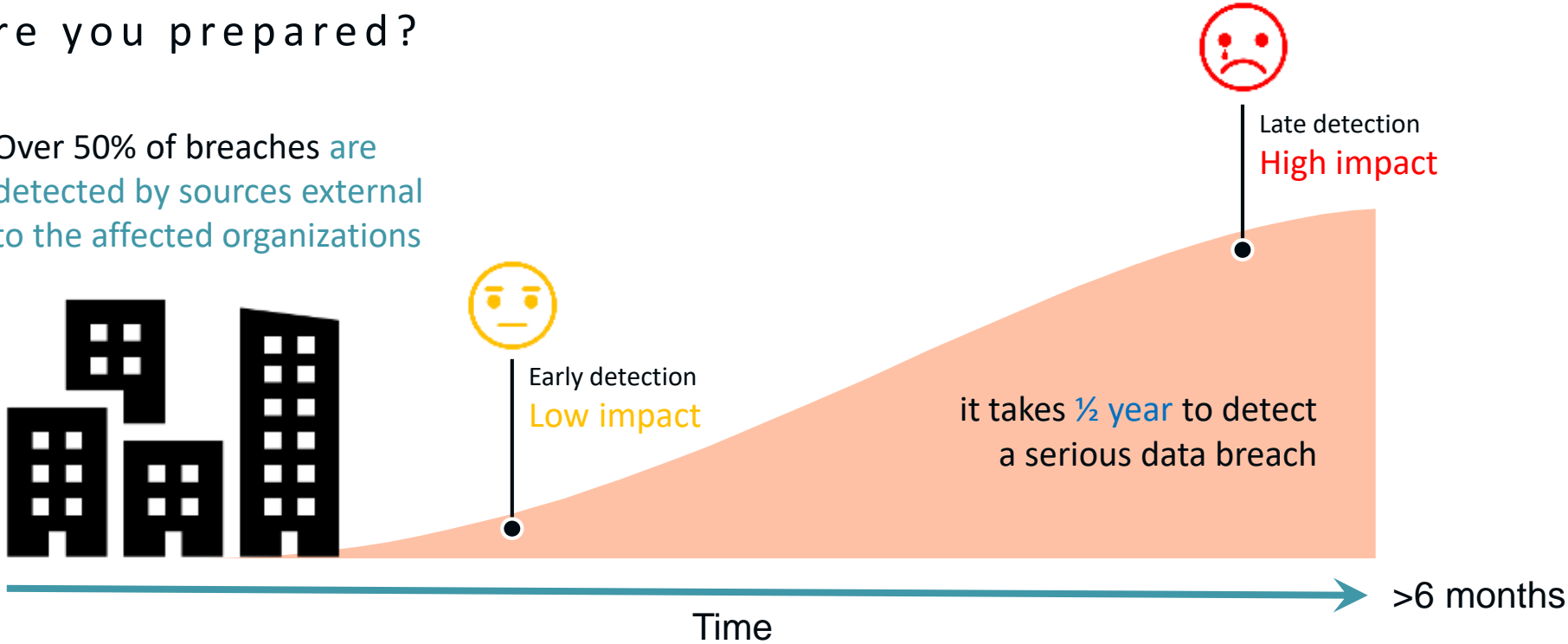
Bitdefender



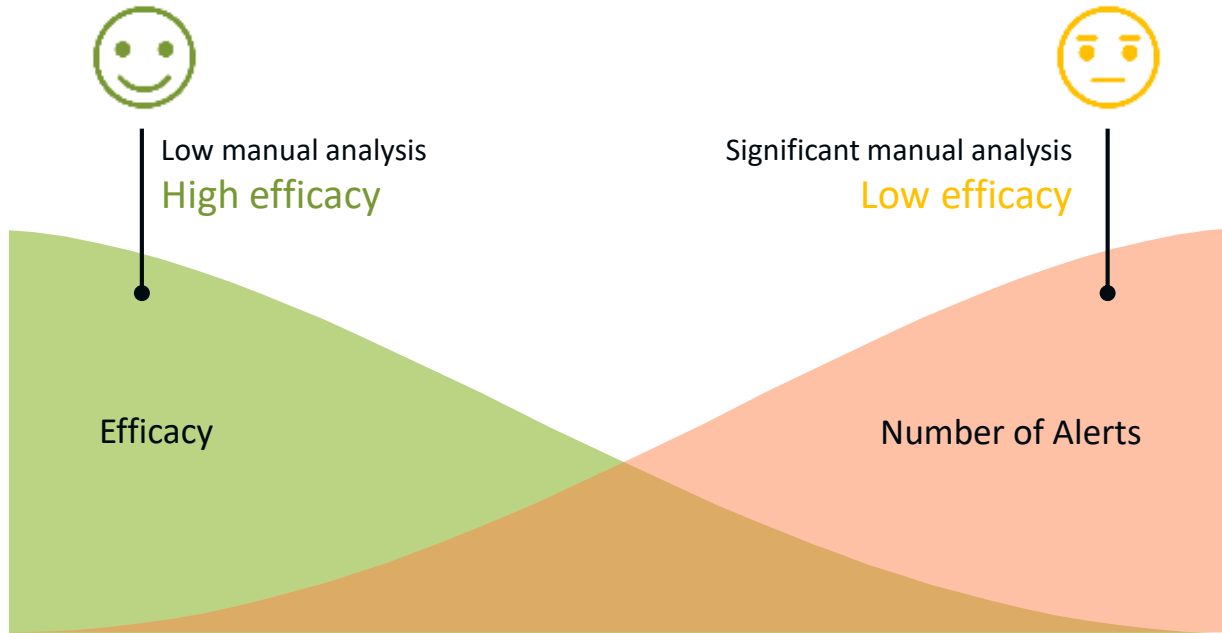
You could be target of an advanced attack

Are you prepared?

Over 50% of breaches are detected by sources external to the affected organizations



SecOps spends time on low value alerts



SOC teams are **under siege** with ever increasing number of security alerts



1 in 3 security alerts is left unchecked

Effective security

depends on incidents visibility and investigation efficacy



Real-time visibility on
security incidents across
entire environment



Effective incident
investigation
and response



Bitdefender Network Traffic Security Analytics

Real-time detection. Automated triage. Complete visibility



Real-time detection of security incidents



Automated triage of security alerts

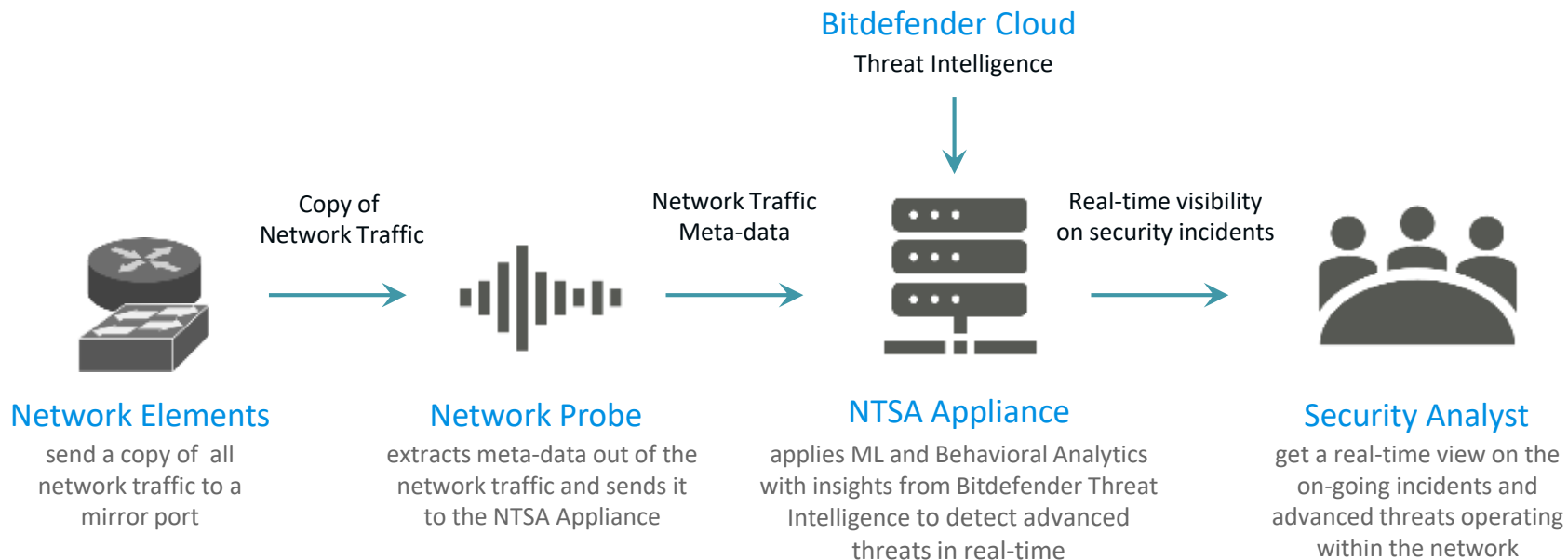


Complete visibility across entire environment



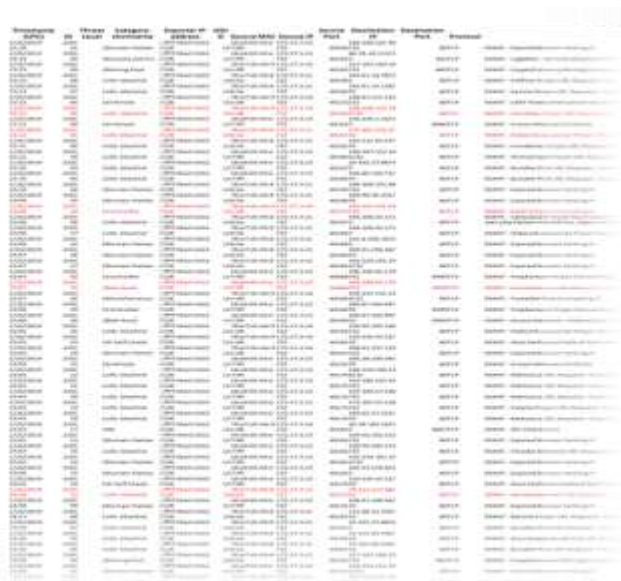
Real-time detection of advanced threats

How NTSA works?



Bitdefender IntelliTriage

From Manual Threat Hunting to Automated Triage



Source	Destination	Action	Severity
192.168.1.10	217.213.41.5	HTTPS upload	High
192.168.1.10	217.213.41.5	HTTPS upload	High
192.168.1.10	217.213.41.5	HTTPS upload	High
192.168.1.10	217.213.41.5	HTTPS upload	High
192.168.1.10	217.213.41.5	HTTPS upload	High
192.168.1.10	217.213.41.5	HTTPS upload	High
192.168.1.10	217.213.41.5	HTTPS upload	High
192.168.1.10	217.213.41.5	HTTPS upload	High
192.168.1.10	217.213.41.5	HTTPS upload	High
192.168.1.10	217.213.41.5	HTTPS upload	High



IntelliTriage enables automated smart triage of network security incidents, generate alerts that provide detailed explanations for incident severity scores and recommends response actions.



Alert Detail Reasoning Detail

1 Upload to valdimir.ru

It is likely **95%** that Office Printer (192.168.1.10) has performed an **HTTPS upload** at **21:35** (CET)

Endpoint device 'Office Printer' with the source IP address '192.168.1.10' has initiated an 'HTTPS' TCP upload of 7.34MB towards the host/hood tagged environment 'Vladimir.ru', hosted on '217.213.41.5' outside of the office hours of 'ODID2' (Sales Office 3rd floor).

The upload connection forwards the Russian based host Vladimir.ru started at 21:35 and the upload was finished at 21:37. This is the first time that a connection was seen to Vladimir.ru from ODID2, and it is the first time that an upload happened after office hours for the endpoint device 'Office Printer'.

Background information on Vladimir.ru (43.2.14)
Hosted at ASN network: 200791
Shared hosting: No
Blacklist item: Yes
Country: Russia

Advice:
It is recommended to take action on the provided alert, take action according to your company security policy.
It is recommended to add 'vladimir.ru' to your Firewall blacklist.
It is recommended to add '217.213.41.5' to your Firewall blacklist as this IP is not a shared hosting environment.
It is highly likely that endpoint device 'Office Printer' is still infected.
It is highly likely that endpoint device 'Office Printer' can be used to traverse through the network.

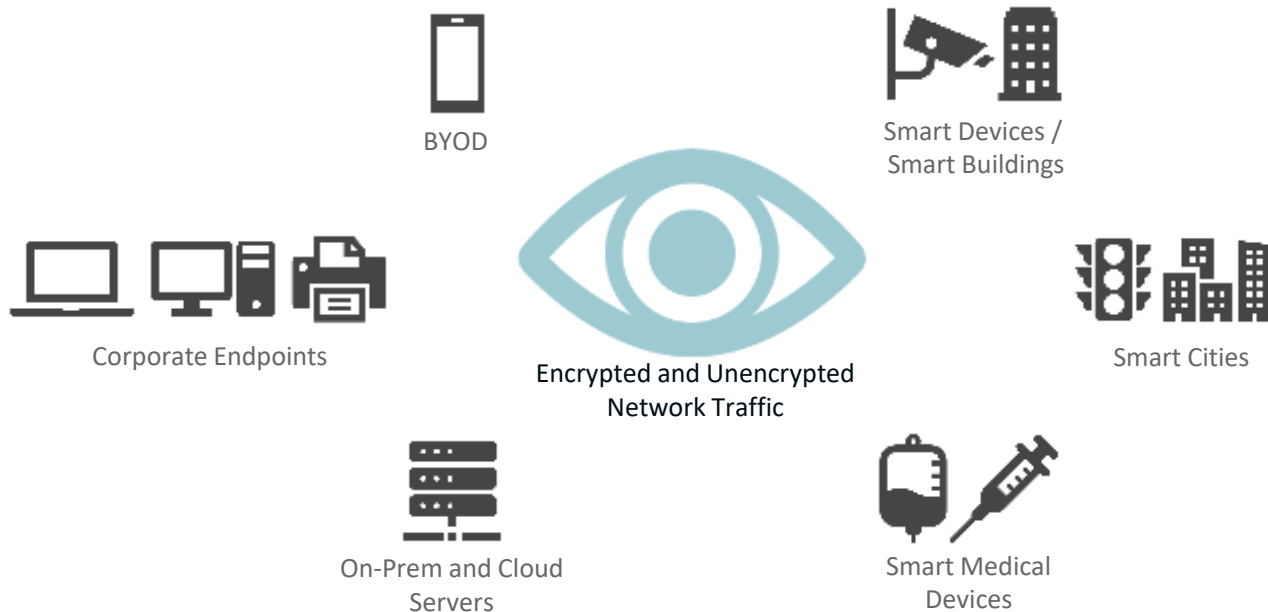
IDS/IPS, NTA, NGFW

Bitdefender NTSA



Complete Visibility on Security Incidents

Across entire environment, for managed and unmanaged devices



Common Enterprise Challenges Resolved



Network Security
Traffic Analytics

Advanced Threat Detection

- Live analysis of all network traffic, including encrypted
- High fidelity alerts using AI/ML & insights from ½ billion nodes

Automated Triage

- Detailed attacker Tactics Techniques & Procedures (TTP)
- Alerts and IR investigations resolved with automation

IOT & BYOD Protection

- Learns & tracks all entities in the enterprise network
- Non-intrusive. No complex log or agent integrations

Compliance

- Helps achieving compliance with PCI, GLBA, NIST, GDPR and others
- Use of meta-data eliminates privacy concerns



The Bitdefender logo is centered on a dark blue background with a complex, abstract pattern of interconnected lines and dots, resembling a network or data structure. The logo itself is the word "Bitdefender" in a white, bold, sans-serif font, with a registered trademark symbol (®) to the upper right of the final letter.

Bitdefender®