Bitdefender Network Traffic Security Analytics

REAL-TIME BREACH DETECTION.
AUTOMATED TRIAGE. COMPLETE VISIBILITY

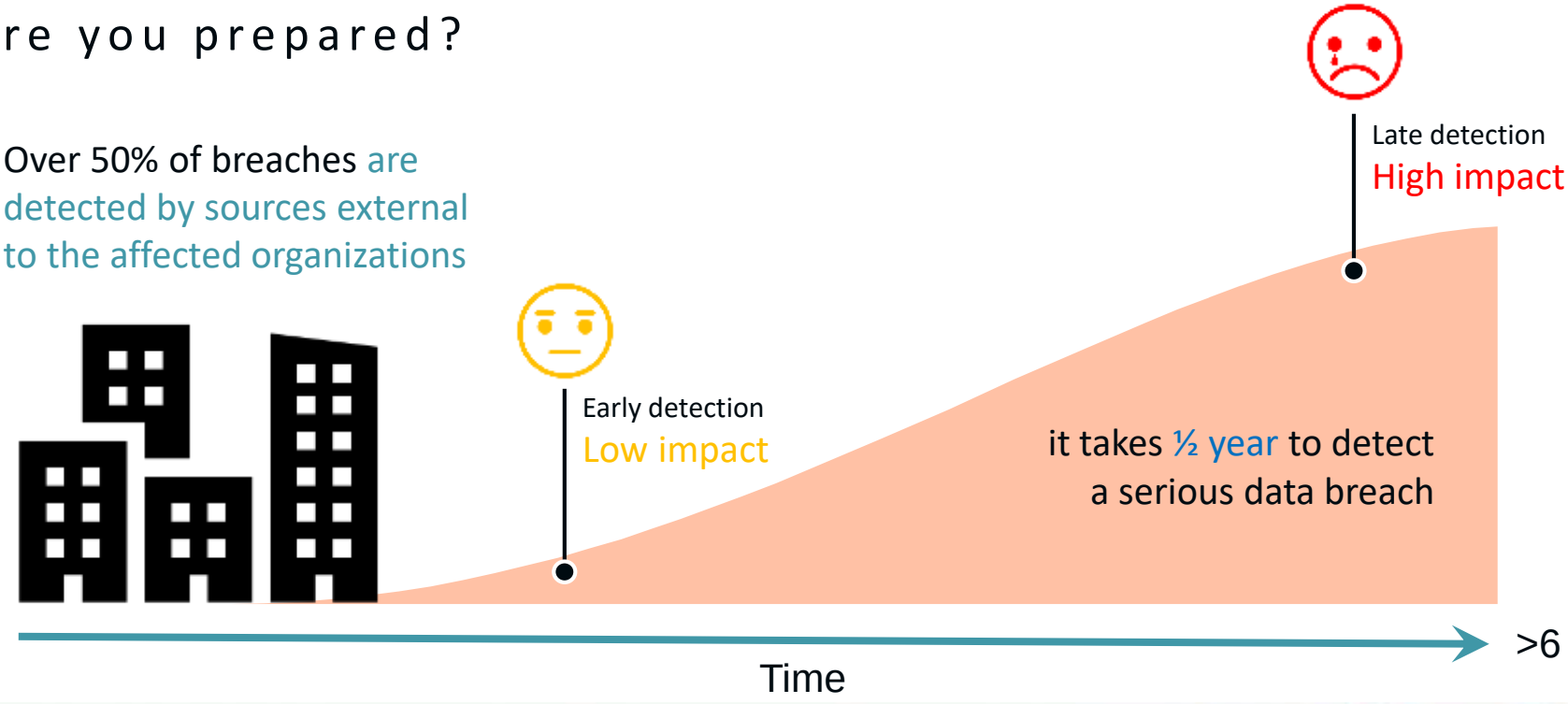
Juan Jesús Merino Torres
National Channel Country Manager

Bitdefender

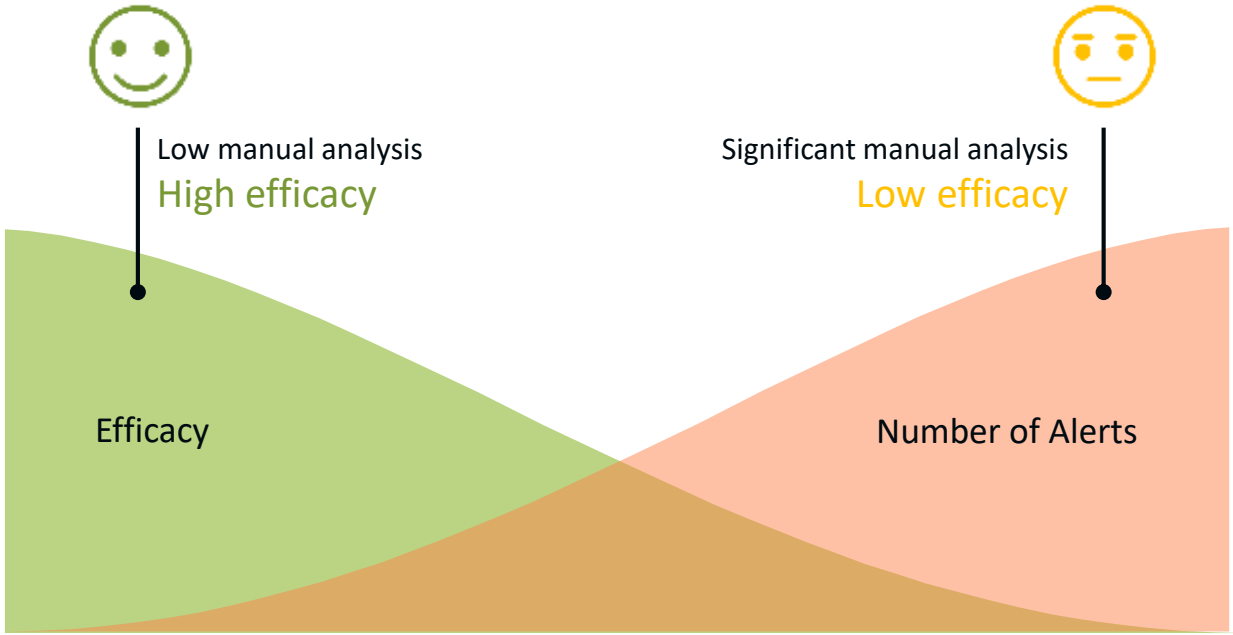
You could be target of an advanced attack

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

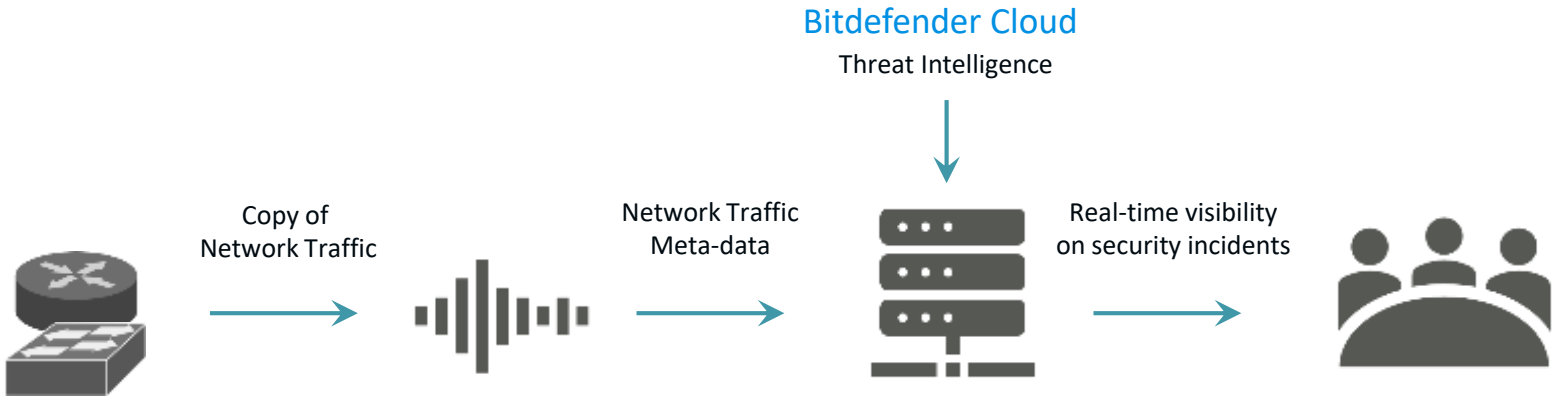
Real-time detection of security incidents

Automated triage of security alerts

Complete visibility across entire environment

Real-time detection of advanced threats

How NTSA works?



Network Elements

send a copy of all network traffic to a mirror port

Network Probe

extracts meta-data out of the network traffic and sends it to the NTSA Appliance

NTSA Appliance

applies ML and Behavioral Analytics with insights from Bitdefender Threat Intelligence to detect advanced threats in real-time

Security Analyst

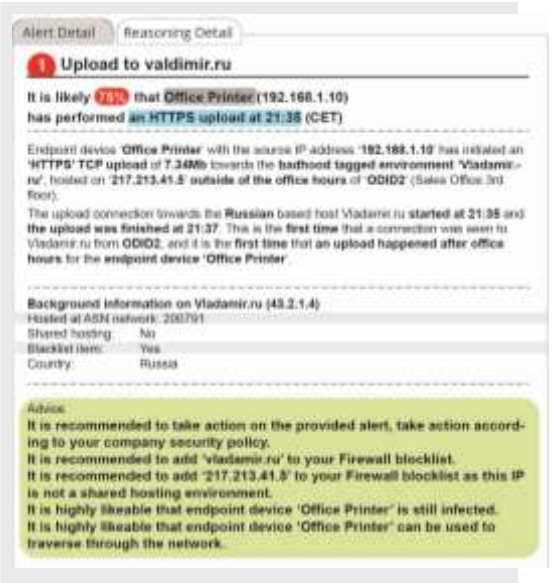
get a real-time view on the on-going incidents and advanced threats operating within the network

Bitdefender IntelliTriage

From Manual Threat Hunting to Automated Triage

IDS/IPS, NTA, NGFW

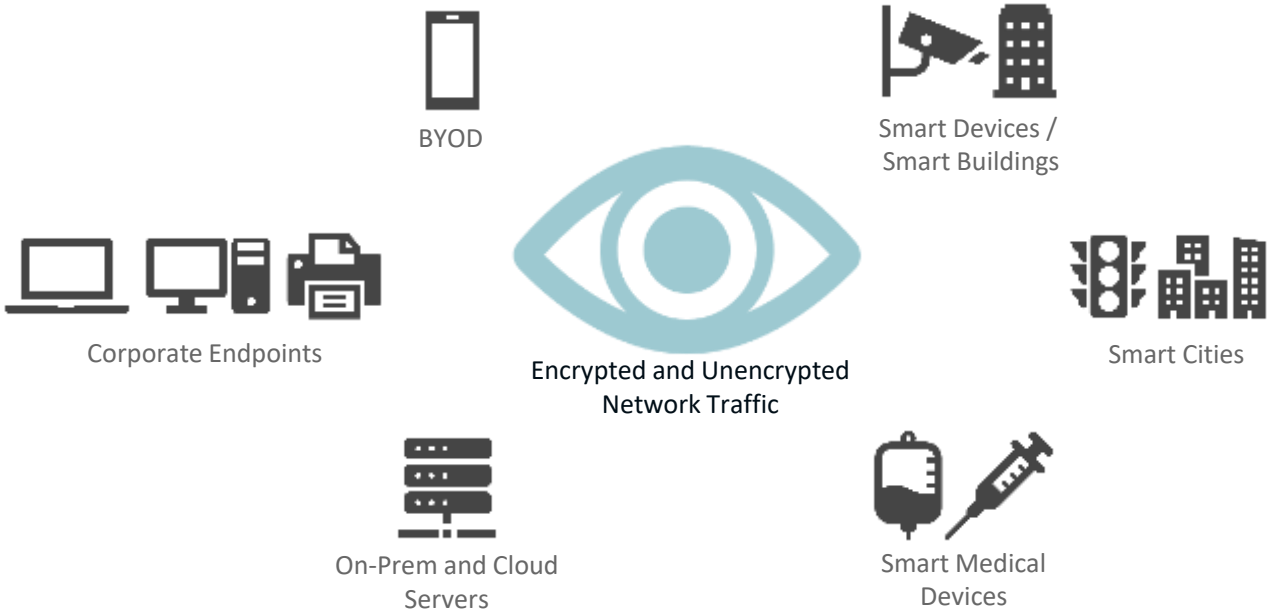
IntelliTriage enables automated smart triage of network security incidents, generate alerts that provide detailed explanations for incident severity scores and recommends response actions.



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