Bitdefender

NETWORK TRAFFIC SECURITY ANALYTICS DATASHEET

Digi Terra ICT SERVICES

Network Traffic Security Analytics

Real-time breach detection and complete threat visibility

Bitdefender Network Traffic Security Analytics is the enterprise security solution that accurately detects advanced attacks in real-time and automates alert triage to provide context and facilitate incident response. It enables organizations quickly detect and fight sophisticated threats by complementing pre-existing security architecture – network and endpoint – with specialized network-based defense.

By using network traffic as a source of reliable information, NTSA detects breaches immediately as endpoint behavior changes once infected. Detection is effective against both generic or advanced persistent threats, known or never seen before. Incident alerts are automatically correlated and triaged for higher security operations efficacy and improved incident investigation and response time.

> "Bitdefender Network Traffic Security Analytics gives IT department full visibility and makes us aware of certain, less desirable things happening in the network"
>
> Leading Automotive & Manufacturing Company

Realtime threat detection for any network device

Provides complete visibility on the threat related activity on all endpoints in the network, independent of type or pre-existing security solutions (corporate- or user-managed devices, network elements, BYOD, IoT).

Save time with Automated security incident triage

Automates security incidents triage by automatically correlating events and generates high-fidelity alerts to improve analysts' threat hunting efficiency.

Hunt for cyber threats with detailed forensics

Provides detailed explanations for every security incident generated with suggested course of actions for improved incident investigation and response.

Leading Cyber Threat Intelligence and Artificial Intelligence

NTSA leverages superior Bitdefender's Cyber Threat Intelligence – collected from 500 million endpoints globally – and combines it with advanced Machine Learning (ML) and heuristics to analyze the network meta-data in real time and to accurately reveal threat activity and suspicious traffic patterns. With automatic security analytics and a focus on outbound network traffic, it reduces noise and provides actionable alerts for security operations.

Digi Terra ICT SERVICES

IntelliTriage – Automates security alerts triage

IntelliTriage, the newest NTSA component, automates the process of security incidents triage to improve incident investigation time and reduce organizational risk with high-fidelity alerts. It also provides recommended remediation guidance on steps to take based on the security incident.

Complex scenario-based learning detects advanced attacks with high accuracy and corelates thousands of security alerts in order to create a clear picture of each incident. IntelliTriage provides detailed explanations for the incident severity score. Recommended remediation actions are also provided to facilitate faster incident response.

> "In identifying the security needs we took into consideration the possible threats from malicious software that might find its way onto the network. For this reason, we were looking specifically for new ways of detecting these threats. So for us the best solution was a security solution that was able to identify network traffic moving from the inside to the outside."
>
> Head of ICT Management for Healthcare Organization

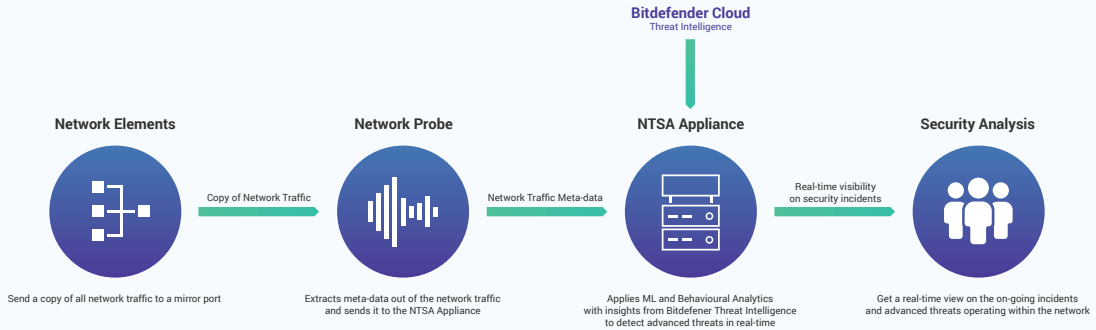
Protection for the Things (IoT) and BYOD in your environment

Enterprise environments are increasingly shared between human operated devices and smart things. While traditional endpoints are typically under scrutiny and well protected, smart things operate in a grey area with limited or no protection. More and more, devices in the network are targeted and used as beach heads during advanced attacks.

NTSA breach detection capabilities extend also to the smart things in the enterprise network. By focusing on the network behavior of endpoints, it can protect devices with limited or no built-in security capabilities and no endpoint security agent running on top (like most IoT devices).

As employees use personal laptops, mobile phones and other devices in business environments, attackers take advantage of them to take corporate information. Securing BYOD increases employee productivity and reduces the risk of exposure of corporate information. NTSA technology helps safeguard organizations from information theft by constantly monitoring and tracking all user and device behavior in real-time and deploying superior threat intelligence. It's agentless, non-intrusive and independent of the operating system.

How it works



Compliance support

Many regulations, GDPR included, require organizations to quickly provide detailed information about malicious activities in the event of breaches. NTSA helps organizations meet compliance requirements by recording information about network data traffic for up to 12 months. The recording contains only meta-data, with no actual payload, and access to recordings is restricted to the Data Privacy Officer role only, eliminating the risk of sensitive information exposure.

Features

Real time and Retroactive detection
Detects breaches by passively checking outbound network traffic in real time for all malicious communication. Applies new threat intelligence elements on recorded meta-data to detect breaches retroactively

Cloud threat intelligence, AI/ML and heuristics
Combines Bitdefender's cloud threat intelligence with real-time network traffic analytics based on AI/ML and heuristics to achieve superior threat detection rates with low false positives

Extended coverage, Complete visibility
Covers all endpoints in the network, independent of type or pre-existing security solutions (corporate- or user-managed devices, network elements, BYOD, IoT). Provides complete visibility and insights into threat-related network activity and endpoint traffic anomalies

Automated Triage, Effective threat hunting
Automates security analytics and reduces noise to improve analysts' threat hunting efficiency and generates actionable alerts to facilitate incident response

Encrypted communication and Privacy
Exclusive focus on traffic meta-data enables analysis of encrypted communications and eliminates privacy issues concerning non-encrypted traffic

Fast deployment, Immediate results
Relies on a simple and flexible architecture (physical or virtualized deployment) with plug-and-play components to deliver results immediately

Integration with GravityZone
Single Sign-On integration with GravityZone on-prem creates a fast and seamless management experience

For more information on Bitdefender NTSA, contact :
Bitdefender Gold & implementation partner Digi Terra ICT Services :
E. sales@digiterra.nl
T. +31 70 4276868