Network Traffic Security Analytics

Real-time breach detection. Autonomous response. Complete visibility

Bitdefender Network Traffic Security Analytics (NTSA) is the enterprise security solution that accurately detects advanced attacks in real-time, provides threat context and triggers autonomous incident response. It enables organizations to 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 threats immediately as the endpoint behavior changes due to an infection. 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. The integration with Bitdefender GravityZone enables autonomous response to quickly remediate security incidents.

> “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 autonomous incident response

Automates security incidents triage for effective incident investigation and automates threat response by integrating with GravityZone to reduce the response time.

360-degree visibility and cyber threats insights

Gives visibility and detailed explanation for the security incidents across the environment. It suggests the course of action for incident containment and improved security posture.

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 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.

IntelliTriage – Automates security alerts triage

IntelliTriage, one of the key elements of NTSA, 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.

Integrated, Autonomous Threat Response

The integration between Bitdefender GravityZone and NTSA enables automated security incident response increases the resilience of the organizations against advanced threats.

For the critical incidents detected in the network, NTSA can automatically trigger GravityZone to investigate the affected endpoints. Depending on the scan result, GravityZone may automatically clean-up and/or quarantine the endpoint(s) in order to effectively contain the emerging threat.

> “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

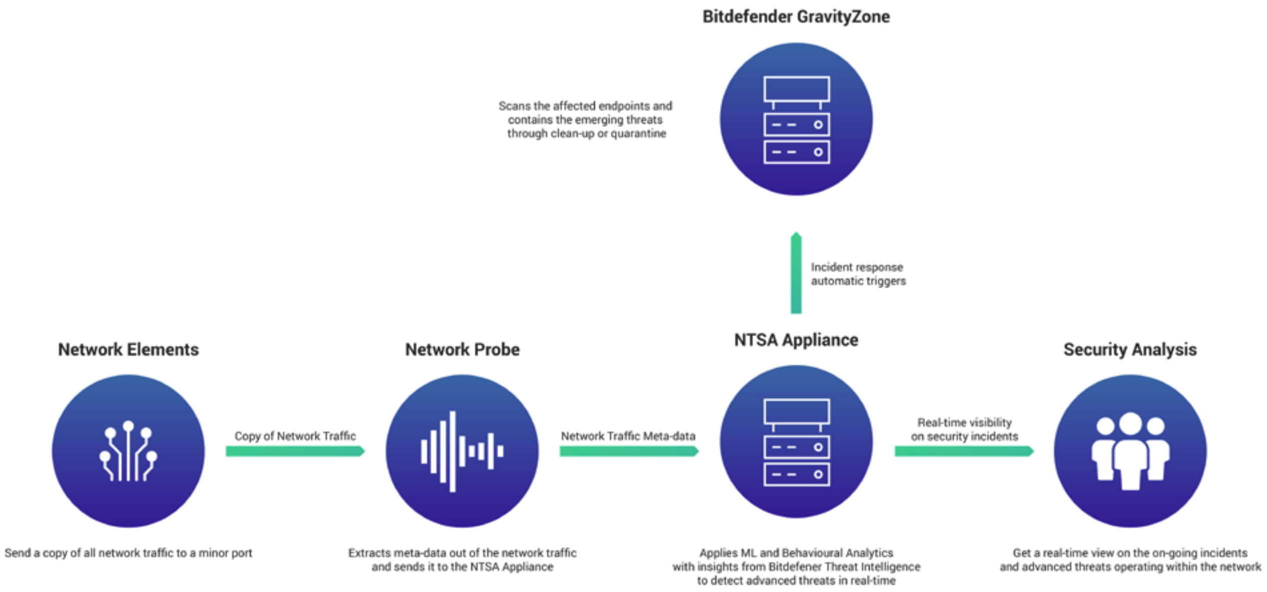
Enterprise environments are increasingly shared between human operated devices and smart things. While traditional endpoints are typically under scrutiny and well protected, smart things operate in a grey area with limited or no protection. More and more, devices in the network are targeted and used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

NTSA architecture and deployment

The NTSA can be easily deployed (plug-and-play), quickly integrated with GravityZone (where appropriate) and provides immediate results. Network performance is not affected in any way, as the solution is out-of-band, analyzing a mirrored copy of the network traffic.


Bitdefender GravityZone
Scans the affected endpoints and contains the emerging threats through clean-up or quarantine
Incident response automatic triggers
Network Elements
Copy of Network Traffic
Network Probe
Network Traffic Meta-data
NTSA Appliance
Real-time visibility on security incidents
Security Analysis
Send a copy of all network traffic to a minor port
Extracts meta-data out of the network traffic and sends it to the NTSA Appliance
Applies ML and Behavioural Analytics with insights from Bitdefener Threat Intelligence to detect advanced threats in real-time
Get a real-time view on the on-going incidents and advanced threats operating within the network

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 detection, 360-degree visibility
Detects breaches by analyzing the network traffic in real time for all anomalous communication. Provides complete visibility and insights into threat-related network activity and endpoint traffic anomalies.

Extended coverage
Covers all endpoints in the network, independent of type or pre-existing security solutions (corporate- or user-managed devices, network elements, BYOD, IoT).

Automated Triage, Automated Response
Automates security analytics and reduces noise to improve analysts' incidents investigation efficiency. Automatically triggers response with GravityZone for critical alerts.

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.

Fast deployment, On-premises or Cloud
Relies on a simple and flexible architecture (physical, virtualized or cloud appliance) with plug-and-play components to deliver results immediately.

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

Integration with GravityZone
The integration with GravityZone creates a fast, seamless management experience and automates security incident response.

For detailed system requirements, please refer to https://www.bitdefender.com/business/enterprise-products/network-traffic-security-analytics.html

Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on.
More information is available at http://www.bitdefender.com.

FOR MORE INFORMATION VISIT: bitdefender.com/business