Network Traffic Security Analytics

Real-time breach detection and complete threat visibility

Bitdefender Network Traffic Security Analytics is an enterprise security solution that accurately detects breaches and provides insights into advanced attacks by analyzing network traffic. It lets 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. Alerts will be generated to inform security operations about endpoint behavioral changes that indicate an advanced attack being deployed or compromised endpoints.

> "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

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.

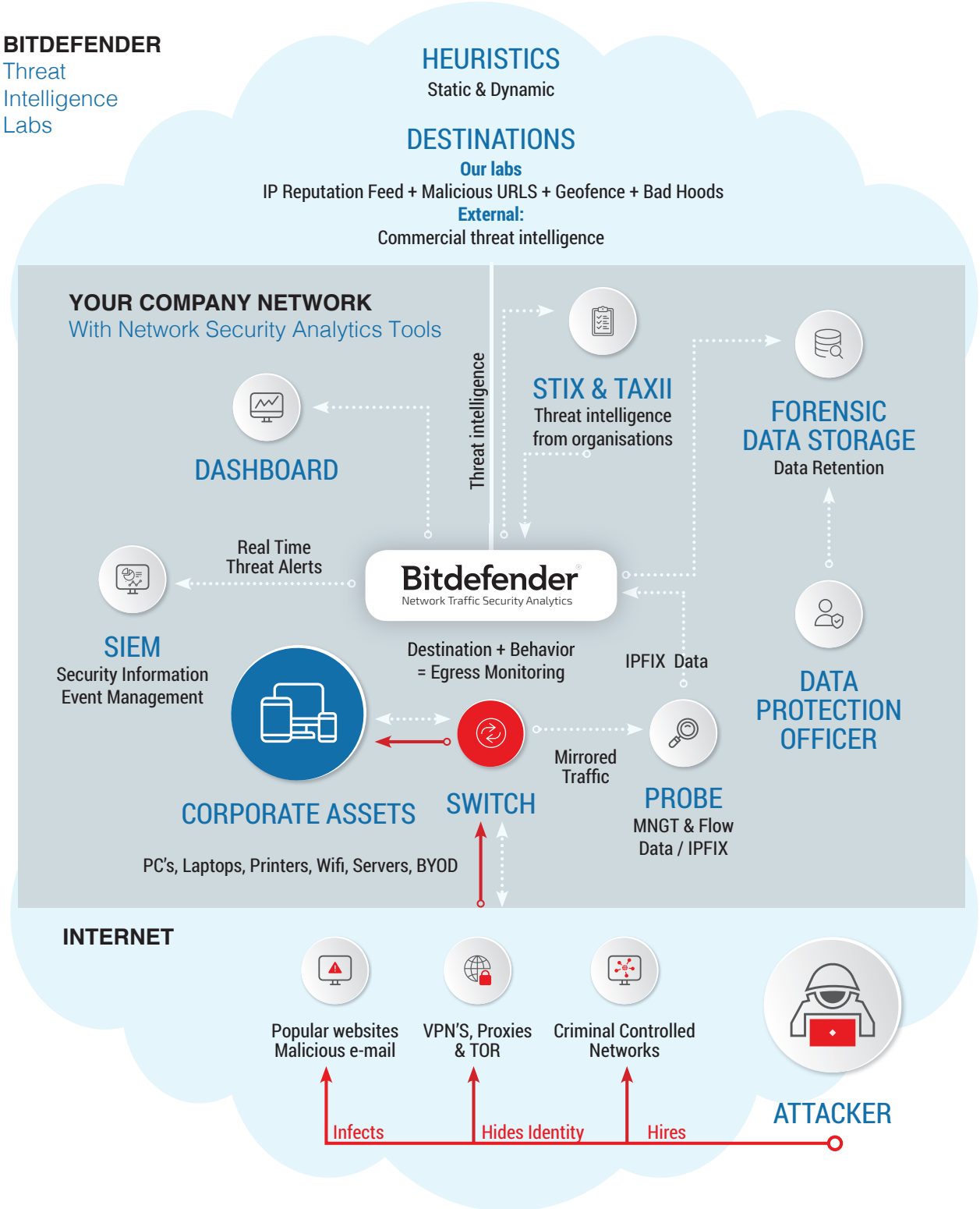
Protection for the Things (IoT) and BYOD in your environment

As employees use personal laptops, mobile phones and other devices in business environments, attackers take advantage of them to reach 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.

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).

NTSA architecture and deployment

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



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.

Key Benefits

Avoid business disruption

- Detects breaches and advanced threats that eluded prevention mechanisms at endpoint or network level
- Provides complete visibility and insights into threat-related network activity and endpoint traffic anomalies
- Combines cloud threat intelligence, ML and behavior analytics to detect the most sophisticated threats

Meet compliance requirements

- Identifies abnormal user behavior or insider threats that may lead to corporate policy violations
- Enables threat hunting and forensics through access to long-term stored data
- Provides fast and easy access to information required by authorities in a 72-hour timeframe after a breach is discovered (GDPR)

Ease of use, fast ROI

- Complementary, easy-to-deploy/easy-to-maintain solution, that delivers immediate results for fast ROI
- Integrations with other monitoring systems allow security automation and quick time to response
- Covers all endpoints in the network, independent of type or pre-existing security solutions (corporate- or user-managed devices, network elements, BYOD, IoT)

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

Reduced noise, 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

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