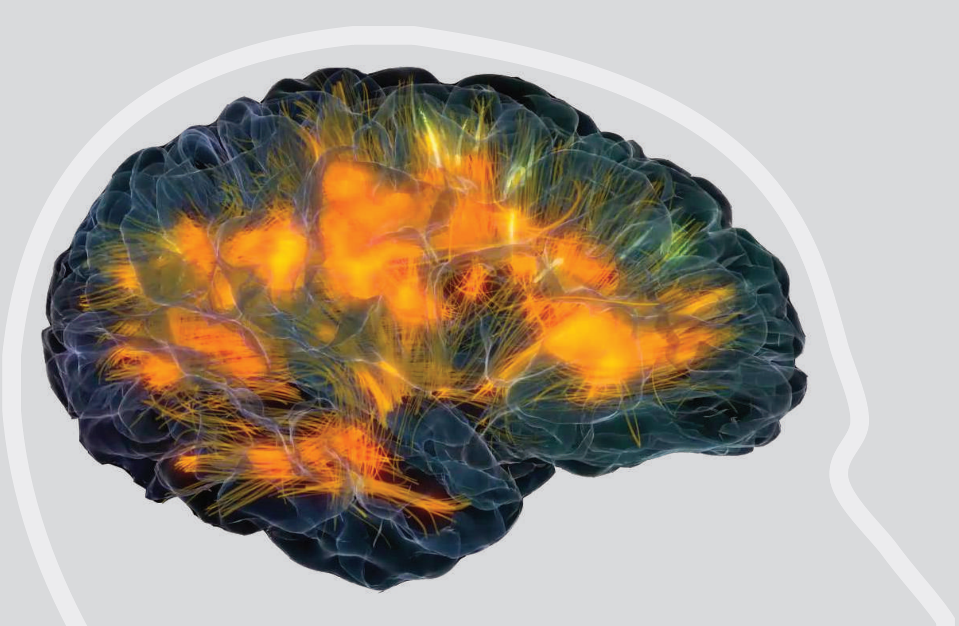


TrustPort

THREAT INTELLIGENCE

Threat Intelligence is a new solution for detection, monitoring and analysis of advanced security events in network traffic. Its unique technology is based on a **new engine of network behavior analysis, advanced machine learning and several other cutting-edge innovations**.

Beyond NetFlow, beyond DPI, beyond signatures...

Threat Intelligence employs **the first specialized protocol for attack detection** as well as tens of newly researched detection algorithms based on advanced mathematical analysis that have never before been used in cyber security. Also, it possesses significantly higher detection capabilities than solutions based on NetFlow analysis, deep packet inspection or detection of known signatures.

Effective Detection of Unknown Threats

Threat Intelligence does not focus on a method of attack nor a piece of malicious code but **symptoms of an attack**. By detecting atomic symptoms of malicious behavior and anomalies in network traffic, it identifies emerging security incidents in their early stages. Thereby, it decreases incident response time, prevents further damage and helps to decrease overall cyber security risks.

Apart from network behavior analysis, Threat Intelligence also processes **additional inputs from signature-based detection, honeypots and incident reports from endpoint security**. This further increases its detection capabilities, reduces false-positive rate and above all, makes Threat Intelligence effective in detection of unknown threats such as

– zero-day attacks

– trojans

– botnets

– internal security incidents

– unauthorized access

– other forms of attacks that are to come in the future.

Security Threats Increase

Despite billions of dollars being invested in security technologies each year, threats continue to evade conventional defenses, compromising sensitive data and wreaking havoc on enterprise networks. Innovations like mobile devices and cloud computing make threat detection incident response even more complicated. Today’s organizations must take a defense-in-depth approach to security and internal network visibility must be a cornerstone of the strategy.

Source: Gartner (Securing Against Advanced Cyber Threats: A Profile of American Cancer Society)

Gartner recommends NBA

After you have successfully deployed firewalls and intrusion prevention systems with appropriate processes for tuning, analysis and remediation, you should consider NBA to identify network events and behavior that are undetectable using other techniques

Not dependent on manual rules

Unlike most anomaly detection and network behavior analysis systems, Threat Intelligence is not dependent on manually set rules (thresholds). Instead, its advanced machine learning automatically generates rules relevant for a particular network. These rules are then gradually automatically adapted as the traffic and threats in the network evolve. This makes Threat Intelligence extremely easy to deploy, maintain and work with.

The network clean & tidy

Threat Intelligence visualizes network traffic and records information on each data flow. Whether in real-time or in retrospect, one can easily identify each flow and find out who uses certain services, network nodes, bandwidth, and other resources.

High usability & low-cost administration

Risk assessment tool analyzes all detection inputs and provides an overview of the most important events and an overall risk rating of the network.

High granularity of user access rules allows users to access their IP only, one specific sub-network, several customized reports, etc.

Effortless deployment – 24 hours after plugging into the network and configuring basic settings, the program will learn your network and begin reporting results. Threat Intelligence is a passive solution therefore, there are no integration problems.

Easy **filtering**, customizable **reports**, intuitive web **interface** & more...

	Market			Dependency	False detection rate	
Solution	launch	Detection mechanism	Perimeter	on updates	F. positive[1]	F. negative[2]
Antivirus, Antispam	1987	Signatures, trivial heuristics, (antirootkits)	End-point	Very high	Very low	Very high
Firewall	1980	No detection – a whitelist of communication attributes (ports, destinations, users, apps …)	Network	Low	Low to High	High
IDS Intrusion detection (and prevention) system	1987	Detection of known signatures in network traffic	Network	Very high	High	High
SIEM Security information and event management	1996	Visualization of causalities between events reported from other infrastructure (IDS, firewall, router, databases, apps …)	Both	Low	Low to medium	Medium
NBAD Network behavior anomaly detection	2004	Predefined rules and thresholds for identification of events that deviate statistically from predicted traffic	Network	Low to medium	High to very high	High
Sandboxing	2006	Execution of suspicious programs and files in secured a virtual environment and subsequent detection of malicious symptoms	Network	Low	Close to zero	Medium
NBA Network behavior analysis based on machine learning	2009	Detection of anomalous behavioral patterns (symptoms) based on artificial intelligence (no signatures and rules needed)	Network	Very low	Medium	Low

[1] False positive = a legitimate item wrongly identified as malicious
[2] False negative = a malicious item wrongly identified as legitimate
[3] E.g. a malicious pdf included in an MS Excel file, included in another MS Word file.

Beyond state-of-the-art technology

Enhanced protocol for sensitive detection. A newly developed Advanced Security Network Metrics protocol is used for monitoring over 60 features (attributes) of each individual data flow. As NetFlow uses only about 10 features, the detection of malicious and other unwanted behavior is much more sensitive and more effective.

Advanced data mining techniques ensure that Threat Intelligence (NBA, IDS) is capable of real-time processing of six times more features of each data flow than NetFlow. By using hardware acceleration, Threat Intelligence has proved to cope with 10Gbps+ and 200.000 flows per second in a single probe & colector configuration. Distributed deployments are prepared for 40Gbps or more.

The Most Modern Machine Learning. For the purpose of automatic generation and adaptation of detection rules (learning from past traffic) and integration of inputs from all detection engines, the most modern machine learning is used. Also, the NBA engine is unique in clear distinction of human behavior and machine behavior.

Automated generation of detection signatures is provided by integrated honeypots with tainted analysis. These honeypots focus solely on recording behavioral characteristics of zero-day attacks exploiting code vulnerabilities such as buffer overflow.

Synergy of various detection engines. Threat Intelligence brings out-of-box integration of the main detection engine – NBA – with additional signature-based detection (IDS) and the honeypots. It is then able to fuse and analyze reported events from these engines and make the detection more effective with fewer false positives.

Grey Cortex NBA engine

The NBA engine employs advanced mathematical analysis in machine learning: Supervised and unsupervised methods of classification, clustering and outlier analysis:

- Models of the network, all subnetworks, hosts, services and individual data flows
- Bayes‘ analysis of transformed features
- Probabilistic mixture models (Gaussian EM)
- Various ad hoc reasoning techniques

Weaknesses	Strengths – detection (prevention) capabilities	Cost of successful circumvention
Detection of common (previously detected) malware only	**Known malware:** Known viruses, worms, spyware and infected files	Low (Change in the targeted structure, change of signatures, IPs, …)
Definition of open ports within internal network boundaries that can be misused	**Prevention of attacks on disallowed services:** Filtering of supposedly untrusted and unwanted communication	Low (Encapsulation of illegitimate communication into legitimate)
Detection of known attacks only (i.e. attacks with known signatures)	**Known risks and threats:** Network attacks with known signatures	Low (Change in the targeted structure, change of signatures, IPs, …)
Dependency on quality of inputs and detection capabilities of other infrastructure Dependency on manually set correlation rules	**Detection of incidents with a possible causal link**: Assistance in highlighting and interpreting complex events that would otherwise be hard to notice or analyze.	High to low (According to the detection capabilities of other infrastructure)
Dependency on predefined and/or manually set rules (thresholds). Inappropriate for detection of sophisticated malware and for networks without easily predictable network traffic.	**Known and predictable risks and threats:** Predictable attacks such as portscans, dictionary attacks, high-volume data transfers, data transfers to unusual geo. locations, usage of disallowed resources (SMTP, DNS, …)	Medium (E.g. by avoiding exceeding the most common thresholds)
Inability to detect malware containing time bombs, logical bombs[3] or requiring user inputs. The sandboxed versions of apps and OS needs to have the same vulnerabilities as the deployed versions.	**Unknown yet predictable risks and threats:** Apps and other files with malicious behavior	Medium to low (Time bombs, logical bombs, waiting for user input)
Effective merely for closing gaps in perimeter-defense infrastructure and faster incident response (less effective in environments with high amount of malicious or other illegitimate traffic)	**Unknown and unpredictable risks and threats:** Detection of outlier behavior, machine vs. human behavior & related symptoms (zero-day attacks, poly- and metamorphic malware, exploits of unknown code vulnerabilities, encrypted communication, improbable behavior)	High

TrustPort
Keep IT Secure

TrustPort is a major vendor of software solutions for secure communication and data protection. Its products protect home to enterprise customers against known as well as unknown threats. According to several benchmarks they excel in antivirus, antispam, and encryption technologies.

TrustPort products have been highly rated in multiple third party tests such as Virus Bulletin that repeatedly confirmed the prominent position of TrustPort in the antivirus industry. TrustPort Antivirus has continously topped the latest Virus Bulletin comparatives and proves to have the best detection capabilities in the world.

Threat Intelligence technology is based on 5 years of university research from the Faculty of IT (Brno University of Technology, Czech Republic) with financial support from the Czech Republic state budget through the Ministry of Industry and Trade. The faculty has been specializing in IT security since 1994. It is well established in network security, voice & video recognition and repeatedly succeeded at NIST challenges.

Technical Specs

Architecture

The TI's enterprise architecture consists of probes and collectors. Probes are used for network traffic analysis and collectors are used to transform these metrics into knowledge. A single TI's distributed cluster can consist of up to 100 collectors and every collector manage about ten probes. Detection capabilities of probes strongly depend on their hardware specification. With TI's hardware acceleration, a single probe can process up to 10Gbps or 2M packets and 200k flows per second. In theory, TI can manage a network of 10Tbps.

Inputs

Network data streams from mirror traffic (SPAN or TAP).

Known botnets, spam sources, TOR nodes and proxies

Outputs

Standard: Web GUI, SIEM (CEF or syslog), customized email reports, pcap files

Optional: Firewall and router management plugins (SNMP, web service, IP tables, IP filter)

Implementation

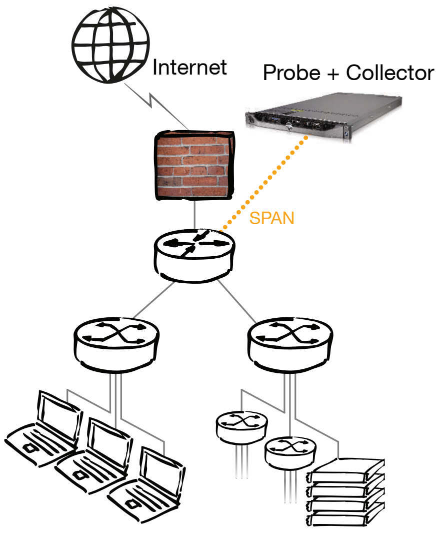
TrustPort Threat Intelligence can be implemented as a hardware appliance or as software on client's HW. Other possibilities include provision of Threat Intelligence in security-as-a-service models and one-off security audit of client's network.

Deployment

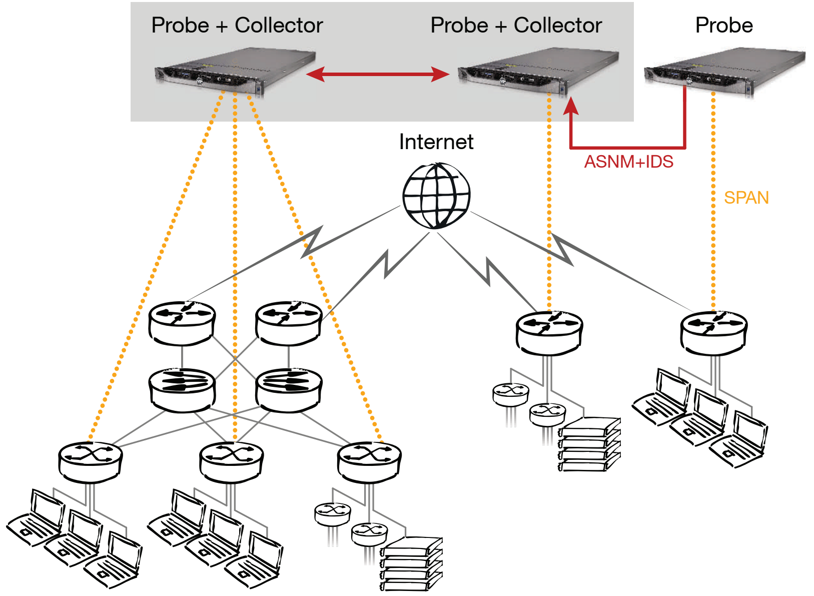
Single deployment with a single network probe and attack processor (collector) in a single HW appliance.

Distributed deployment with a number of collectors and probes sharing knowledge about the network traffic and threats (for monitoring geographically distant locations and/or processing high traffic volumes)

Threat Intelligence
Single Port Deployment



Threat Intelligence Security Cloud



TrustPort
THREAT INTELLIGENCE

Purkynova 101, 612 00 Brno, Czech Republic +420 541 244 471, ti@trustport.com