TrustPort
THREAT INTELLIGENCE

SOLVE THE SECURITY OF YOUR NETWORK ONCE FOREVER!

ADVANCED MONITORING

Cybercrime activities are mainly focused mainly on the weakest points of all Internet users. For today´s companies, it is still difficult to ensure sufficient monitoring and protection of information systems which should prevent misusage of possible leaks of sensitive data. Examples and experience from the past show us that resisting modern cybernetic attacks is difficult also for large international corporations. Common security technologies usually become obsolete quickly and they cannot resist new threats. Their maintenance and operation is usually very demanding on resources. It is necessary to use modern detection methods and tools for successful elimination of modern and increasingly sophisticated virtual threats.

MODERN TECHNOLOGIES

A new security solution named TrustPort Threat Intelligence moves tracking and detecting of modern attacks to the level of network environment (Internet entry point, internal router, etc.). It is a security SW solution designed to monitor, analyse and report of undesirable events within a network operation, based on most modern IT technologies.

The target of a network operation analysis is not only to recognize known attacks and malware, but specifically the detection of newest network worms, trojans, botnets, zero-day attacks, internal attackers, non-authorized access and other undesired events. It provides detailed information about security aspects of the network operation of a company in real time. It offers an overview of the whole network where it shows, how and by whom individual elements are used, how they are connected and by which ports and protocols they are communicating. It also enables statistical evaluations of network communications and visualizations of individual flows.

COMPLEX SOLUTION

TrustPort Threat Intelligence evaluates network behavior of users, services and whole subnetworks. It creates automatic long-term models of behavior – communication of stations and servers – which become the base for the sophisticated process of detection of anomalies. From these models, the solution is able to recognize real attacks, or a malware presence thanks to advanced methods of flow analysis using artificial intelligence. You can correlate reported incidents with outputs of other integrated security technologies - IDS (Intrusion Detection Systems) and central antivirus software. Network administrators can use the well-arranged web interface for network monitoring with a quick overview of incidents, which enables risk assessment of stations and elimination of false positive detections.

ADVANTAGES

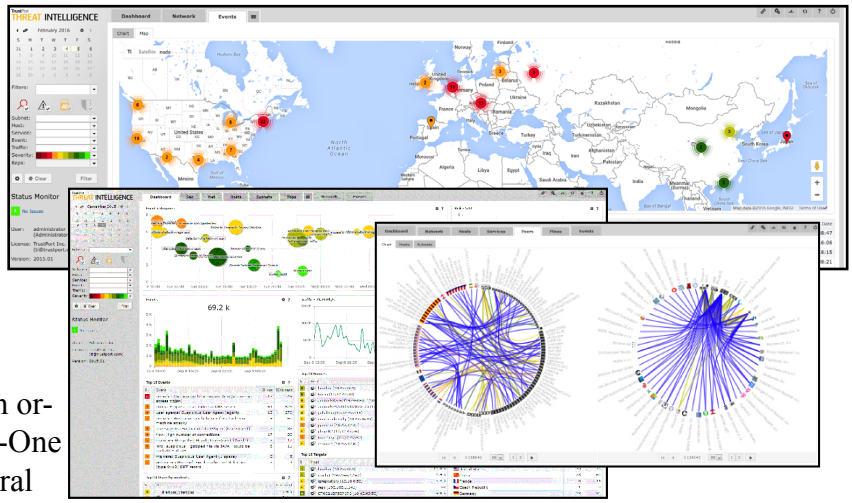
- Security monitoring and network visualization
- Protection against modern attacks
  APT (Advanced Persistant Threats)
  RAT (Remote Access Trojan)
  Zero-Day threats
- All-In-One solution
- Decreasing of costs of network administration
- Modern technologies and methods of A. I.
- Easy implementation

COMPONENTS

- Network Behavior Analysis (NBA)
- Intrusion Detection System (IDS)
- Network Risk Assessment
- Flow Monitoring
- Antivirus

TrustPort

THREAT INTELLIGENCE



INNOVATIVE
UNIQUE
PROGRESSIVE

TECHNOLOGY

TrustPort Threat Intelligence can also be deployed in organizations with several branches. Except the All-In-One device, separated probes which send data to the central analyzer are also available. Installation in a virtual environment is also available.

Expanded flow recording protocol

TrustPort Threat Intelligence uses its own expanded protocol ASNM (Advanced Security Network Metrics) for analysing network operations. This enables significantly better and more effective detection than standard flow protocols (e.g. NetFlow), however these can also be processed.

Latest elements of advanced artificial intelligence

The detection engine for behavior analysis itself is made of several modules based on modern artifical intelligence methods. It uses tens of recently published and newly developed detection algorithms, which are completed with methods of reverse learning from reported failures (false positive detections).

Complex database processing

The system is based on full relational processing of all data, which enables users to filter desired parameters completely and efficiently.

High-speed deployment

TrustPort Threat Intelligence can be deployed with no loss of the detection sensitivity even into networks with an average operation higher than 10 Gbps.

Distributed deployment model

TrustPort Threat Intelligence can also be deployed also in organizations with several branches. Except the All-In-One device, separated probes which send data to the central analyzer are also available. Installation in a virtual environment is also available.

Easy filtering

High level of filtering options enables easy and quick access to desired information.

High granularity of users´ competencies

The system administration enables giving a user various competencies, e.g. accessing only one IP address, or one overview within the Dashboard.

Critical infrastructure

The TrustPort Threat Intelligence solution was developed for all areas where protection of network and data is important.

Other features

Advanced reporting, latest technologies, highly secured configuration.

WWW.TI-SECURITY.COM

TrustPort
Keep IT Secure

TrustPort, a. s.
Purkyňova 2845/101
612 00 Brno

T: +420 541 244 471,
F: +420 541 235 038
E: info@**trustport.com**