

Attacks against computer network from inside, most time by your own employees or using stolen identities, could not be adequately detected by current security technologies.

At this moment current technologies are working on 'deny' principle. This approach cannot be effectively used in an open environment such as LAN or WAN. Deny method is hardly usable as defense against unknown threats. Why? You simply cannot deny something you do not know as you are not able to identify what exactly shall be forbidden.

Let's take a look into stories taken from real life.

John expects that he might lose his job really soon, as the company he is working for, is under a reorganization process. Such uncertainty leads him to question, how can he 'insure' himself against possible dismissal, especially he has been hard working for this company for whole 15 years. He decided to focus on business contacts, unique technology as well as he is interested what compensations other people got during dismissal. As sales man, he already has access to important information such as company technologies and customer contacts, so he easily copies all the huge amount of information to his notebook hard drive transferring everything to his home computer later.

Later on he finds out, that one of the accountants has problems with Internet access. He phone calls to this accountant acting as IT technical support staff a manages to get her password. After that he successfully accesses accounting software, where also all employees data are stored and easily gets information about wages and compensations of other employees. Additionally just in case he copies considerable amount of data from company accounting system he considers useful.

Company had installed many of the latest security devices for network protection, but somehow missed the protection against attacks from internal network.

This intrusion was discovered, after court case between the employee and the company had started.

Was there even a small possibility how to avoid this? Well, yes ! One of the most effective methods is definitely so called Behavioral Analysis of applications, users and devices. When we look deeper into the example above, it is clear that such analysis would find out several anomalies. User accessed the file server with incomparably higher intensity, exploiting most of its resources, downloading huge amount of data. Accessing accounting system using stolen identity can also be detected, because of non-standard user behavior as he was accessing the system from quote different computer and unusually high resources usage on the system would also be detected.

Let's have a look on another real world example:

IT administrators in one banking institute had been granted

unrestricted access to almost every single system, including customer database containing sensitive personal data. One of them Mr. J.K. had been asked by his old high school friend currently working at marketing agency, whether he could help him. It was necessary to obtain a list of wealthy clients for marketing campaign. Mr. J.K. copied most of data containing personal clients information from customer database to DVDs and handed them over to his friend. He was aware that somebody might find out, so he carefully deleted any relevant information from system auditing access to the database.

Bank got suspicious after longer time period, just after considerable number of clients publicly complained about recent intrusive advertisement. Some clues advised that there is some connection with Mr. J.K., but it was impossible to prove anything to him, just because he carefully deleted all the compromising entries from database log.

Similarly as in the first example the bank had implemented most of the modern security solutions, but again unfortunately they did not expect their own employees may also represent threat to system security.

Was it possible to avoid this case as well? Utilizing behavior analysis correlating network events with application events certainly yes, as the main aspect of this data leak is the fact, that there was access to the database evident in the network traffic, but there was no corresponding log entry in the database itself. Additionally unusually high resource usage of the database by the employee, that was quite different from his usual daily work, would be again considered as an evident anomaly and reported to appropriate internal safety department of the bank.

We can clearly see on the above examples, that users always changed their behavior significantly. For common security systems such activity would not be even suspicious, as every access to any of these resources, applications was realized according to the users permissions and roles, even when using stolen identity.

For behavior analysis system, which is profiling actual behavior over a long time period, such activities will be detected and reported as a major security incident.



MyNetScope® is complete solution for network monitoring, long term storage of network traffic statistics, centralized statistics processing, behavioral analysis, provides tools for

network infrastructure over-watch and administrative-organizational background for security team. As a first solution it implements bidirectional flows standard and methods to detect attack against network services on the network level (network based methods) without the need to process transferred data.

Network Flows Monitoring

- Powerful autonomous solution of real-time NetFlow v5/v9 monitoring
- From 10Mbps to 10Gbps link speed support
- IPv4, IPv6, VLAN and MPLS support
- L2 a L3 invisible.
- Provides primary data for following applications:
 - Network traffic analysis
 - Users and services monitoring
 - Internet access over-watching
 - Network and connectivity planning
 - Peering and SLA checking
 - Electronic communication law compliance
 - Undesirable behavior detection
 - Anomaly detection
 - Security incident investigation process

Centralized Long Term Network Traffic Statistics Storage

- Powerful NetFlow statistics collector for any number of monitored network points
- From 1TB to 50TB storage capacity
- Central database for long-term network traffic statistics storage
- Analysis and additional reevaluation platform
- Network availability and stability overview platform

Centralized Statistics Processing

- Bidirectional Flows standard implementation
- Pre-defined rules for undesirable behavior detection
- Pre-defined rules for anomaly detection
- Ready for extension with additional behavior and anomaly detection rules
- Network security improved with ability to detect additional internal or external breaches
- Dictionary attacks detection
- Long term behavior profiles creation
- Hidden and unwanted services revelation
- Security incident classification according to classes and importance
- Security incidents history

Behavioral Analysis

- Highly optimized behavioral analysis of:
 - users
 - network devices

- individual applications
- network in global
- Undesirable behavior detection
- User activity including services usage monitoring
- Correlation between network events with application logs

Network Infrastructure Insight

- Network events overview in real time
- SNMP based monitoring of network devices
- Scheduled and summarized reporting
- Long-term statistics analysis including resolution to individual computers and users, applications and conversations

Advanced Network Traffic Analysis

- Automatic DNS integration with intelligent cache
- Filtering based on selectable criteria
- Network port number translation to service names.
- Additional information about services and known threats
- Network diagnostics integration (ping, traceroute, nmap) and additional information (WHOIS)
- Security incident investigation
- Effective network problems solution
- Detailed information about behavior of selected device or network user
- Global network situation view

Administrative-Organizational Background for Security Team

- Text storage as dokuwiki standard
- Access to changes in RSS format
- Ticketing system, automatic emailing of changes
- Security know-how centralization
- Extensive evidence of security incidents
- Overview of steps taken during incident resolution
- Methodology and best practices for security teams

Technical Support and Software Updates

- Phone or email support 8x5
- Remote assistance and device configuration
- Security consulting services
- Software and firmware updates
- Behavior patterns updates

MyNetScope® solution grows together with the customer, compared to common products, especially it is ready for extension of number of monitored network points. MyNetScope® provides market best price to performance ratio including low administrative cost. Average time required for the implementation is mostly around several hours and it does not require highly specialized professionals for day to day work.