BALABIT

CONTEXTUAL SECURITY INTELLIGENCE


# USER BEHAVIOR ANALYTICS FOR TELECOMMUNICATIONS PROVIDERS

How to uncover attacks and save money with the approach of fraud detection?

**Telecommunications operators are at the center of data security risk today. Having millions of subscribers, telco providers store a huge amount of highly confidential personal data, which are very appealing for infocriminals and identity thieves.**

# HOW CAN A TELECOMMUNICATIONS OPERATOR REDUCE THE CHANCE OF BREAKDOWNS AND ENSURE BUSINESS CONTINUITY IN A BIG DATA ENVIRONMENT?

*"FCC has just issued its first fines over data security, slapping phone carriers TerraCom and YourTel with a total of $10 million in penalties for storing their customer info in the clear."*

Engadget

*"An individual or individuals with authorized access took and shared the records… for more than 70 million phone calls…Of those records, 14,000 were calls between prisoners and their attorneys"*

The Verge

*"A hacker has acquired the records of 15 million T-Mobile customers and people who had applied for credit. The breach, which affected two years worth of records, occurred at Experian, the vendor that processes T-Mobile's credit applications."*

USA Today

*"Vodafone hacker accesses 2 million customers' banking data. A person with insider knowledge stole data including names, addresses, birth dates, and bank account information."*

Bloomberg

This is only a short selection of the biggest data breaches in the last few years. These prove that telecommunications operators are one of the favorite targets of cybercriminals. If you don't want to become well known about a huge data breach, you must find the right arms to efficiently improve your IT security.

## Main IT-related challenges

### Protecting client, billing and call data

- Tons of compliance regulations
- Monitoring of data access is a must

### Great need for business continuity

- Too much control-based defenses may be counterproductive to business continuity
- Early detection and time to respond is crucial

### Thousands of networking devices managed by countless 3rd party operators

- It would be important to know who is doing exactly what

### Huge IT infrastructure

- Scalable security solutions are needed

# How can Blindspotter help you?

## Detect malicious insiders and external attackers as early as possible

Blindspotter lowers the impact of potential breaches and provides an effective defense against Advanced Persistent Threats. Attackers using valid user credentials, or malicious insiders who want to steal company data show different behavior patterns from regular users. Blindspotter is able to detect the level of deviation from normal user activity in near real-time and alert the security team. Moreover, it can also help discover the leakage of confidential data, such as personally identifiable information.

## Show what outsourced colleagues are doing in the system

Often there are several 3rd party employees working at a telecommunications operator, accessing the operator's IT systems and data. Blindspotter helps you spot if any of these users are doing something potentially dangerous by providing a unique, behavior based overview of how they are interacting with the IT system.

## Enhance security without hindering business continuity

Every minute of service downtime may cost millions in arrears of revenue and falling brand value to telecommunications operators. The reduction of preventive controls imposed by IT security solutions supports business flexibility, but this comes at the cost of decreased overall security. In such cases, only detection-based security technologies – such as Blindspotter – may provide the sufficient level of defense without impeding the required flexibility.

## Focus on what is important

Critical systems and privileged users are among the biggest risks for telecommunications operators. The machine learning algorithms and pluggable architecture of Blindspotter helps you to focus on exactly these critical systems, users and data by analyzing the related activities and detecting anomalies and other suspicious activities in near real-time.

## Service continuity: detect anomalies which could lead to outage

For the development of new digital services, providers need to collect, store and protect an increasing amount of (potentially sensitive) customer data. While developing these services, business agility is of high importance, and the employees working on these solutions need to be able to have access to all the data and systems that enable them to perform their job. This urge to provide greater access to data conflicts with the need to keep the data secure. Applying preventive security controls on a "least privilege" and "need to know, need to do" basis is becoming increasingly more challenging. Blindspotter is the ideal solution in such a situation: it is able to reduce this extended risk by providing state-of-the-art analytics and monitoring capabilities and defending against malicious access of sensitive data without preventing legitimate users from doing their job.

## Detect potentially risky events in the IT infrastructure

Behavior analytics can be used to detect unusual, and potentially risky events that are not necessarily attacks. Detecting account sharing or if a user account is used for automated tasks enables security analysts to investigate such activities and decide if these require further action to prevent abuse or a potential data breach.

## Optimize the efficiency of security teams

Blindspotter increases the effectiveness of security teams by providing a prioritized list of security events, so security analysts can focus on the most important incidents. In addition, Blindspotter gives an overview of how different services are used within the company, and thus help discover the access privileges the individual users should be granted.

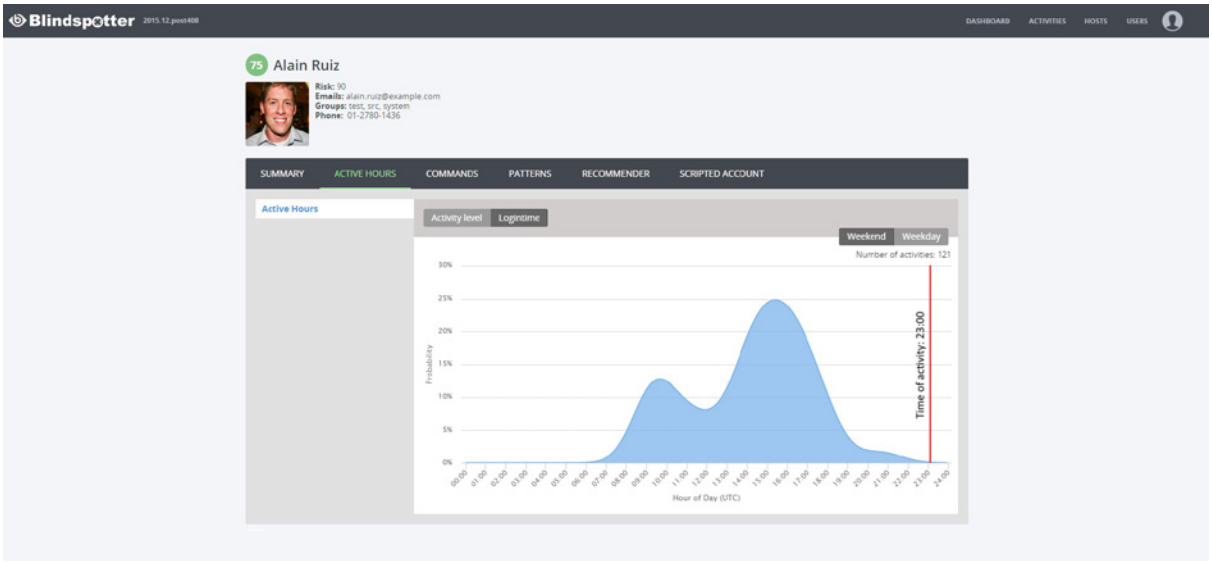
## Scalable solution for big data environments

Telecommunications operators store and manage significantly more data than most other enterprises. For this reason, they require an easily scalable security solution which is able to optimally work in big data environments as well. Blindspotter is designed to tackle this challenge.

# How does Blindspotter work?

Blindspotter works similarly to fraud detection methods in the telecommunications sector. By detecting deviations from normal behavior and assigning a risk value, Blindspotter helps companies focus their security resources on important events, and also allows them to be strategic about the placement of security controls, yielding greater business efficiency. It identifies users' "digital footprints", processes them using unique sets of algorithms, and generates user behavior profiles that are continually adjusted using machine learning. With advanced monitoring across every aspect of an IT system, Blindspotter helps protect sensitive and critical data from potential security breaches, from both internal and external attackers.

Blindspotter maximizes the benefit of User Behavior Analytics methods when deployed together with Shell Control Box, which records the details of user activities like a CCTV camera. In this case, Blindspotter is able to analyze not only biometrics information, such as mouse movements and typing dynamics, but the used applications and issued commands of the users as well, even precisely recognizing any credential theft or privilege misuse. With these world-class monitoring tools, Blindspotter gives a better visibility of user behavior, enabling security teams to better focus on unusual user activities, thus improving efficiency and lowering risks.




## Telecommunications references

Telenor

Facebook

France Telecom – Orange

Fon

Bouygues Telecom

MTS Ukraine

Magyar Telekom