



# PALLADION

Fraud Detection and Prevention

A self-learning, scalable solution that is optimized for fraud detection and prevention.



# the problem

Current fraud prevention solutions are limited

They detect attacks only when a lot of damage has already been done. They are only partially automated requiring human time, intervention and can mean oversights. They don't cover all types of fraud and cannot keep up with the evolving methods of attack.



# the solution

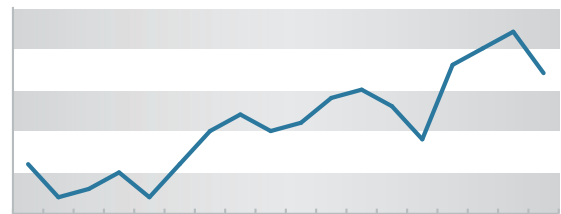
Faster, smarter and more flexible

Fraud Detection & Prevention is a solution which uses a technology difficult to scam - automated behavioural analysis. Built upon PALLADION, it's a passive monitoring system collecting real-time information about all calls, users, customers, trunks and more.

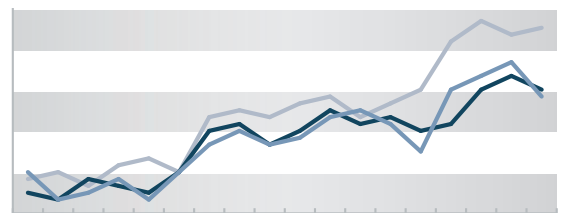


## How it works

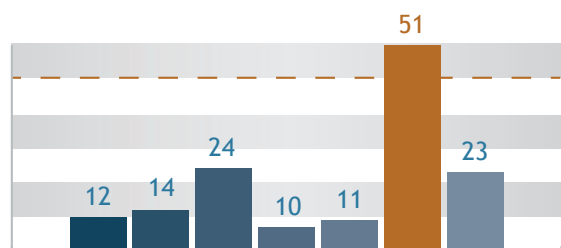
- 1** PALLADION monitors all participants in a network, and reports current encrypted usage info to the Fraud D&P system.
- 2** Fraud D&P automatically learns behavioral patterns of all participants over time.
- 3** Fraud D&P applies scores to all calls and all participants based on customizable rules.
- 4** Fraud D&P calculates, scores and blocks those beyond the current threshold derived from the ongoing analysis.
- 5** Calls are blocked by using APIs of existing network elements from vendors such as Broadsoft and Acme Packet.



monitoring



behavioural analysis



score assignment and threshold

## key features

It's self-learning, no need to configure specific behavioral patterns

It can stop fraud as it happens

### PALLADION fraud detection & prevention

It works fully agnostic of the method of attack

It's a scalable solution optimized for fraud detection and prevention

It's a flexible light-weight deployment, provided as a solution on top of a PALLADION installation

## Smart Fraud Detection Scenarios

Fraud D&P detects individual and combined fraud scenarios for each user. Applying weights to each scenario avoids false positives and allows for detecting actual fraud cases quickly. Some of the main examples include:

### Burst Calls

The amount of calls and number of minutes spoken for a particular user rises to a multiple of what is usual for the same customer on similar type of day and time of day.

### Working Hours

An enterprise which usually only generates calls during their business hours, i.e. from 9am to 5pm, on business days suddenly has a burst of calls on weekends and/or evenings.

### Unusual Destinations

From a phone account that usually has mostly national or low cost national calls now generates a large amount of calls to expensive destinations

### Varying Locations

A user who usually makes calls from IP addresses out of the US makes many calls from IPs out of unusual countries such as China, Afghanistan etc.

## Contact us

### Head office

Berlin

IPTEGO

Wittenbergplatz 1  
10789 Berlin • Germany

Phone +49 30 2038 999 00

Fax +49 30 722 398 987

E-mail [INFO@IPTEGO.COM](mailto:INFO@IPTEGO.COM)

Web [WWW.IPTEGO.COM](http://WWW.IPTEGO.COM)

### EMEA

Milan office

Gino Bettoni

Phone +39 33 51 33 41 90

E-mail [gino.bettoni@iptego.com](mailto:gino.bettoni@iptego.com)

### Americas

Boulder office

Richard Jobson

Phone +1 (719) 488-1003 ext.101

E-mail [richard.jobson@iptego.com](mailto:richard.jobson@iptego.com)