\Orchestrating a brighter world NEC

# InGUARD

## NEC'S BUILT-IN TOLL FRAUD DEFENCE

## PRO-ACTIVE APPLICATION AGAINST TOLL FRAUD ATTACKS - 'ON DUTY' 24/7/365

**InGuard is an effective, low cost solution to help protect a business against the rise of toll fraud attacks.**

Toll Fraud is a fraudulent attempt by a hacker to gain unlawful remote access to a phone system. Attacks are often highly organised from an automated server. Once accessed, fraudulent calls are connected and over a period of time they can run up call charges of potentially thousands.Typically, these occur out of office hours and are usually discovered after the event when it's too late and businesses are left to cover the costs.

The vast majority of businesses are considered vulnerable to these attacks and most networks and phone systems have only basic toll restriction features. Although no solution can provide 100% protection, this application is strongly recommended.

### USER & BUSINESS BENEFITS

**Peace of mind** with an effective toll fraud defence

**'On duty' 24/7/365** and reacts instantly to a toll fraud attack

**Tailored specifically** to the needs of your business and call patterns

**Zero maintenance** solution which 'sits in the background', until any alerts are triggered

**Easy to use,** alerts are easily switched off if telephone useage is legitimate

**Acts as a strong deterent** to internal telephone abuse

### AT A GLANCE

- Effective toll fraud defence for SV9100 and SL2100 users
- Highly cost-effective
- Low maintenance

**As one of NEC's InApps solutions, features include:**

- Built-in/embedded application
- Browser-based and available 24/7
- No extra PC/Server required - data is stored on the CPU
- Save on hardware costs and IT maintenance

nec.com.au

## INGUARD OVERVIEW

InGuard is an embedded application that runs on the CPU of the PBX.

- The application helps to prevent toll fraud by monitoring call records
- It has the ability to alter the system programming to prevent extensions from dialling out and certain numbers from being dialled
- 'Rules' are then created and when they are breached, further calls can be blocked
- Custom rules can be created for departments that make lots of calls or known safe dialled numbers

## HOW INGUARD WORKS

All call activity is monitored 24/7 and any suspicious call activity is detected instantly. This results is one of two automatic alerts:

- An 'alert only' email sent to designated recipients
- In more severe cases an 'alert and block' which prevents any further call activity instantly
- The emails provide call information explaining why a call or calls were considered to be suspicious

Once checked, if the call activity is legitimate the restriction can be removed simply by replying to the email and your business communications continue as normal.

## BESPOKE SETTINGS FOR A BUSINESS

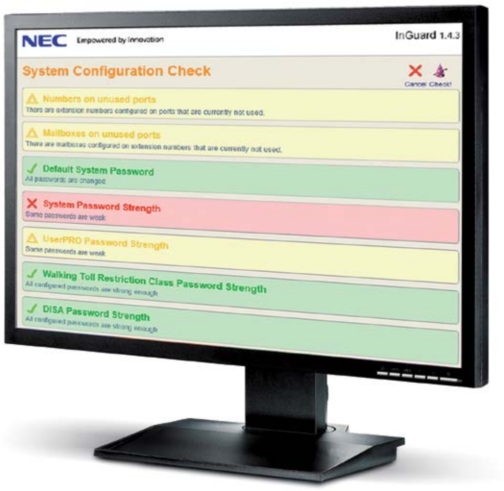
The simple set-up of Toll Fraud is based around your businesses specific call patterns, i.e. office hours, public holidays, length of a call, excessive calls rates, etc.

- From these parameters a set of rules are created – and if a rule is broken, an alert is sent
- Not only does this detect a suspected toll fraud attack, it can also help prevent internal abuse of the system
- Amends to rule settings (e.g. changes in office hours) can be made remotely via a browser for easy administration

## HEALTH CHECK FEATURE

This feature helps to make sure the system is setup in a secure way, not leaving it susceptible to toll fraud.

- The Health Check feature looks at the configuration of the PBX and carries out numerous security checks
- A report is produced indicating any potential areas of vulnerability - these can be reviewed by the installer to determine if the system is securely configured
- Green indicates a feature is well configured and secure
- Yellow means the configuration may have potential security considerations and should be reviewed
- Red is a security risk and this issue should be remedied



NEC Empowered by Innovation InGuard 1.4.3

System Configuration Check

⚠ Numbers on unused ports
There are extension numbers configured on ports that are currently not used.

⚠ Mailboxes on unused ports
There are mailboxes configured on extension numbers that are currently not used.

✓ Default System Password
All passwords are changed

✕ System Password Strength
Some passwords are weak

⚠ UserPRO Password Strength
Some passwords are weak

✓ Walking Toll Restriction Class Password Strength
All configured passwords are strong enough

✓ DISA Password Strength
All configured passwords are strong enough

## SYSTEM REQUIREMENTS

- SV9100: R5 for Inguard, R8 for InGuard health check
- SL2100: R1 for Inguard, R1.5 for InGuard health check

**For more information:**

www nec.com.au ✉ contactus@nec.com.au ☎ 131 632

**Corporate Headquarters (Japan)**
NEC Corporation
www.nec.com

**Australia**
NEC Australia Pty Ltd
www.nec.com.au

**North America (USA)**
NEC Corporation of America
www.necam.com

**Asia Pacific (AP)**
NEC Asia Pacific
www.sg.nec.com

**Europe (EMEA)**
NEC Enterprise Solutions
www.nec-enterprise.com

NEC Australia Pty Ltd reserves the right to change product specifications, functions, or features, at any time, without notice. Please refer to your local NEC representatives for further details. Although all efforts have been made to ensure that the contents are correct, NEC shall not be liable for any direct, indirect, consequential or incidental damages resulting from the use of the equipment, manual or any related materials. The information contained herein is the property of NEC Australia Pty Ltd and shall not be reproduced without prior written approval from NEC Australia Pty Ltd.

NEC