



Marcel Schick  
Sales Engineer @ Boll  
**P**rivileged **A**ccess **M**anagement

# SUPERMARKET

EXIT

FRUITS



19.99



sale





# Wer war es?

1. Die Mitarbeiter?
2. Der Lieferant?
3. Ein Kunde?



# Was nun?

1. Das Lager wird abgeschlossen
2. Es bekommen nur die richtigen Mitarbeiter einen Schlüssel
3. Das Lager wird Videoüberwacht
4. Bei neuen Lieferungen ist immer ein Mitarbeiter vor Ort

Hurra, kein Diebstahl!





**FUDO**  
SECURITY

by Wheel Systems Inc.





2004

2005

2006

2012

2015

2016

GRÜNDUNG

WHEEL CERB AS

WHEEL CERB AS  
FOR BANKING

WHEEL FUDO  
PSM

WHEEL LYNX SSL  
INSPECTOR

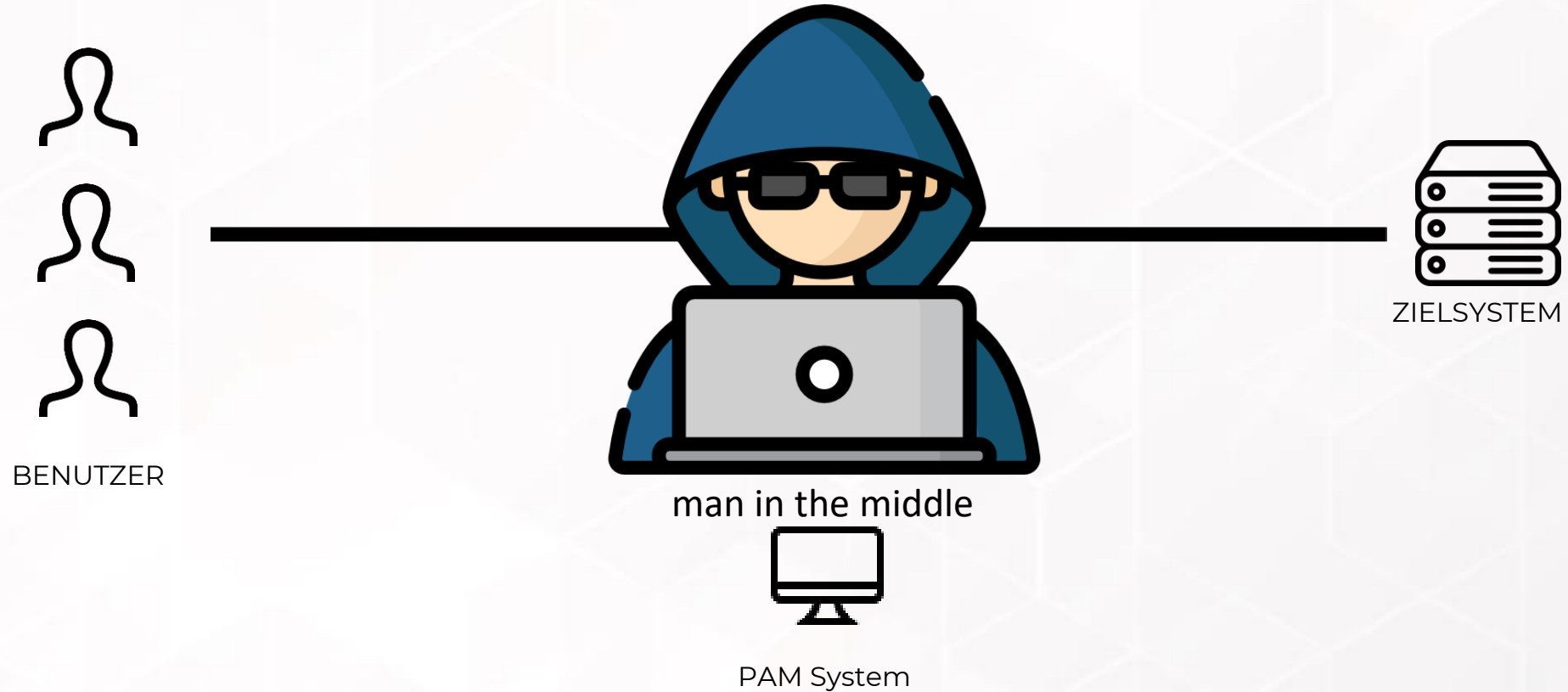
WHEEL FUDO  
PAM



# Was macht PAM?

1. Direkter Zugriff auf System nur über PAM möglich
2. Nur berechtigte Mitarbeiter bekommen Zugriff
3. Alle Sessions werden aufgezeichnet
4. Externe Mitarbeiter können beaufsichtigt werden

# It's not a cyber attack, it's a feature!



# GIF mit Beispiel Verbindung Web

The screenshot shows the FUDO web interface. At the top, there is a navigation bar with the FUDO logo, an 'ONLINE HELP' link, and a user profile for 'marcel'. Below this is a filter bar with tabs for 'All', 'Requestable', and 'Webclient'. The 'All' tab is selected. The filter bar contains several dropdown menus for 'Account name', 'Protocol', 'Server / Pool name', 'Server / Pool descripti...', and 'Host/Mask:Port', along with a 'Search case sensitive' toggle. The main content area displays a list of five accounts, each with a 'Password history' button. The accounts are:

Account name	Protocol	Server / Pool name	Host/Mask:Port	Additional Info
HTTP_User	HTTP	Portainer	172.217.16.163...	External   Address (1)
KundenTest	RDP	Testkunde	192.168.66.107/...	Webclient   Subnets (2)
RDPUser	RDP	TestRDP	192.168.100.10...	Webclient   External   Address (1)
SSHUser	SSH	TestSSH	192.168.100.11...	Webclient   External   Address (1)
testAccount2	RDP	TestRDP	192.168.100.10...	Webclient   External   Address (1)

At the bottom of the page, there is a pagination control showing '1' and a footer with 'Session time: 14 : 58' and 'Copyright © 2023 Fudo Security'. The Windows taskbar is visible at the very bottom of the image.

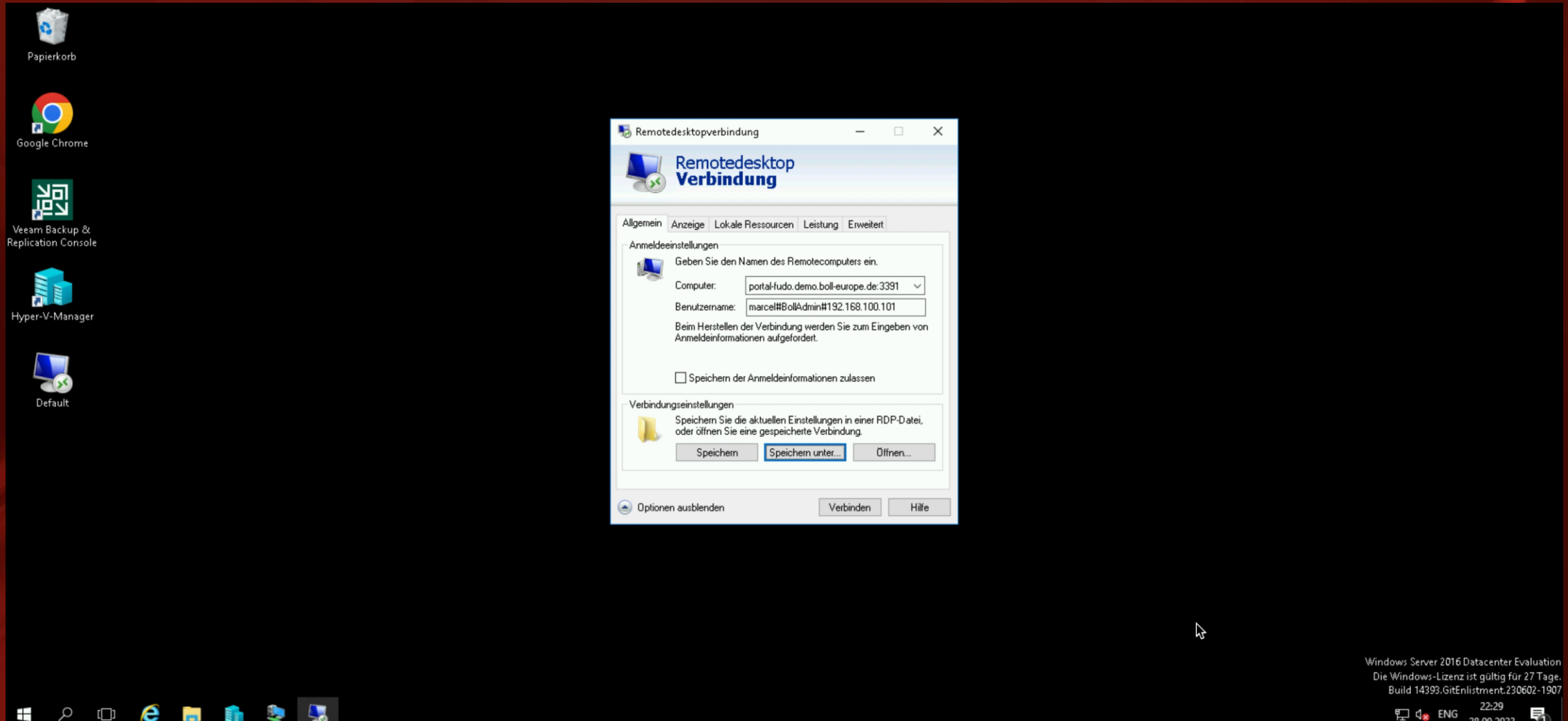
# GIF mit Beispiel Verbindung Native

The screenshot shows the FUDO web interface. At the top, there is a navigation bar with the FUDO logo, an 'ONLINE HELP' link, and a user profile for 'marcel'. Below the navigation bar, there are tabs for 'All', 'Requestable', and 'Webclient'. A search bar is present with filters for 'Account name', 'Protocol', 'Server / Pool name', 'Server / Pool descripti...', and 'Host/Mask:Port'. A 'Search case sensitive' toggle is also visible. The main content area displays a list of five accounts, each with a 'Password history' dropdown menu. The accounts are:

Account name	Protocol	Server / Pool name	Server / Pool descripti...	Host/Mask:Port	Additional Info
HTTP_User	HTTP	Portainer		172.217.16.163:...	External   Address (1)
KundenTest	RDP	Testkunde		192.168.66.107/...	Webclient   Subnets (2)
RDPUser	RDP	TestRDP		192.168.100.10...	Webclient   External   Address (1)
SSHUser	SSH	TestSSH		192.168.100.11...	Webclient   External   Address (1)
testAccount2	RDP	TestRDP		192.168.100.10...	Webclient   External   Address (1)

At the bottom of the page, there is a pagination control showing '1' and a footer with 'Copyright © 2023 Fudo Security'. The session time is '15:00' and the system language is 'ENG'.

# Web? Native bitte!



marcel#BollAdmin#192.168.100.101

# 2FA

- Papierkorb
- Google Chrome
- Veeam Backup & Replication Console
- Hyper-V-Manager
- Default

Remotedesktopverbindung

## Remotedesktop Verbindung

Allgemein Anzeige Lokale Ressourcen Leistung Erweitert

Anmeldeeinstellungen

Geben Sie den Namen des Remotecomputers ein.

Computer: portal-fudo.demo.boll-europe.de:3391

Benutzername: marcel-otp#BollAdmin#192.168.100.101

Beim Herstellen der Verbindung werden Sie zum Eingeben von Anmeldeinformationen aufgefordert.

Speichern der Anmeldeinformationen zulassen

Verbindungseinstellungen

Speichern Sie die aktuellen Einstellungen in einer RDP-Datei, oder öffnen Sie eine gespeicherte Verbindung.

Speichern Speichern unter... Öffnen...

Optionen ausblenden **Verbinden** Hilfe

# Access Request

portal-fudo.demo.boll-europe.de/accounts?page=1&main=all&query=

Zabbix Billigflüge nach B... 958562-17-2023... 958562-17-2023... 958562-17-2023... Alle Lesezeichen

FUDO ONLINE HELP marcel-otp

All Requestable Webclient

Account name Protocol Server / Pool name Server / Pool descri... Host/Mask:Port Search case sensitive

RDPUser	RDP	TestRDP	192.168.100.1...	Webclient External Address (1)
SSHUser	SSH	TestSSH	192.168.100.1...	Webclient Address (1) Requests

< 1 >

Session time: 14 : 52 Copyright © 2023 Fudo Security



# Policies

The screenshot shows a terminal window titled 'TestSSH' with the user 'SSHUser'. The terminal output includes:

```
Session wird nach DSGVO aufgezeichnet. Bei Fragen: tech@boll.ch wenden
Connection reason: Updates installieren
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-72-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Do 28. Sep 21:09:34 UTC 2023

System load:  0.08349609375   Processes:            219
Usage of /:   44.0% of 28.37GB Users logged in:      0
Memory usage: 48%           IPv4 address for eth0: 192.168.100.112
Swap usage:  10%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Erweiterte Sicherheitswartung (ESM) für Applications ist nicht aktiviert.
233 Aktualisierungen können sofort angewendet werden.
Zum Anzeigen dieser zusätzlichen Aktualisierungen bitte »apt list --upgradable« ausführen

13 zusätzliche Sicherheitsupdates können mit ESM Apps angewendet werden.
Erfahren Sie mehr über die Aktivierung des ESM Apps-Dienstes at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

*** System restart required ***
Last login: Thu Sep 28 21:09:34 2023 from 192.168.1.230
raitadmin@mail:~$
```

At the bottom of the terminal window, it says 'Session time: 14 : 59' and 'Copyright © 2023 Fudo Security'.

# Einfach nur Video? Nein, Rohdaten!

The image shows a remote desktop session of a Windows 10 desktop. The desktop background is the standard Windows 10 blue wallpaper with the four-pane logo. On the left side, there are four desktop icons: 'Papierkorb' (Recycle Bin), 'WindDreieck' (Windmill), 'Microsoft Edge', and 'Remote Desktop Manager Free'. The taskbar at the bottom contains the Start button, a search bar with the text 'Suchen', and several application icons including a tree icon, Edge, File Explorer, and Mail. In the bottom right corner of the taskbar, there is a weather widget showing '15°C Teilw. bewölkt' and a 'Leave session' button.

Overlaid on the bottom of the desktop view is a video player interface. It includes a progress bar with a play/pause button on the left and a '0:04:50' timestamp. To the right of the progress bar are several control buttons: 'Time limit', 'Info', 'Details', 'Share', 'Disable retention', 'Terminate', 'Leave', and 'Pause'. Below the video player is a 'Live view!' label and a timeline with markers at 0:04:20, 0:04:25, 0:04:30, 0:04:35, 0:04:40, 0:04:45, and 0:04:50. A mouse cursor is visible over the timeline, and there is an 'Add comment' button below it.

# Rohdaten = Viel Speicher?

MP4 1080p 3GB/Stunde (170 Stunden)

RDP 1080p 218MB/Stunde (2348 Stunden)

SSH nur Zeilen!



# Weitere Funktionen

- KI-Erkennung des Users durch Peripheriegeräte
- Automatische Passwortrotation
- Timestamping mit Zertifikat
- Hardwareverschlüsselung / NATO Zertifizierung

# Nicht nur insider thread!

- Kontrolle von externen Dienstleistern
- Schulung
- Dokumentation
- Sicherer Remotezugang

“The elephant in the room”



# PAM und NIS2?

## Welche Risikomanagementmaßnahmen sind zu treffen?

### 10 Risikomanagementmaßnahmen (Mindestmaßnahmen):

- Konzept Risikoanalyse und Sicherheit für Informationssysteme
- **Bewältigung von Sicherheitsvorfällen**
- **Business Continuity** und Krisenmanagement
- **Sicherheit der Lieferkette**
- Sicherheitsmaßnahmen bei **Erwerb/Entwicklung/Wartung** von IKT
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- **Cyberhygiene** und **Schulungen** zur Cybersicherheit
- **Kryptografie** und ggf. Verschlüsselung
- Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle**
- **Multi-Faktor-Authentifizierung**



© BLUE PLANET STUDIO | STOCK.ADOBE.COM





# Will haben!



	<b>F1002</b>	<b>F3002</b>	<b>F5000</b>	<b>Fudo Virtual Machine</b>
Format:	2U	3U	4U	VMWare, Xen, HyperV, VirtualBox, KVM
CPU & RAM:	Intel® Xeon® E5-1650 v4 (15M Cache, 3.60 GHz) 6 cores, 32GB ECC RAM	2x Intel® Xeon® E5-2640 v4 (25M Cache, 2.40 GHz) 10 Cores, 64GB ECC RAM	2x Intel® Xeon® E5-2690 v4 (35M Cache, 2.60 GHz) 14 Core, 128GB ECC RAM	3GHz CPU 4core, 32GB
Storage: raw / usable	12x 2TB HDD 24TB / 18.2TB double redundancy	16x 6TB HDD 96TB / 71.8TB triple redundancy	36x 8TB HDD 288TB / 261TB triple redundancy	min. 2TB
Expansion	FC card	multiple FC	multiple FC	
SSD cache	2x 500GB	2x 960GB	2x 960GB	recommended
Network	4x 1GbE	4x 1GbE optional 10GbE fiber	4x 1GbE optional 10GbE fiber	2x NIC ( or 1 with VLAN)
Performance				min. 1000 IOPS
concurrent sessions (*)	up to 100	up to 200	up to 300	add 10 IOPS per user

(\*) average 30% FullHD 32bit RDP and 70% terminal sessions



Vielen Dank!