Marcel Schick

Sales Engineer @ Boll

Privileged **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.

WHEEL SYSTEMS

CERB

CERB BANKING

FUDO

LYNX

FUDO

2004 — GRÜNDUNG

2005 — WHEEL CERB AS

2006 — WHEEL CERB AS FOR BANKING

2012 — WHEEL FUDO PSM

2015 — WHEEL LYNX SSL INSPECTOR

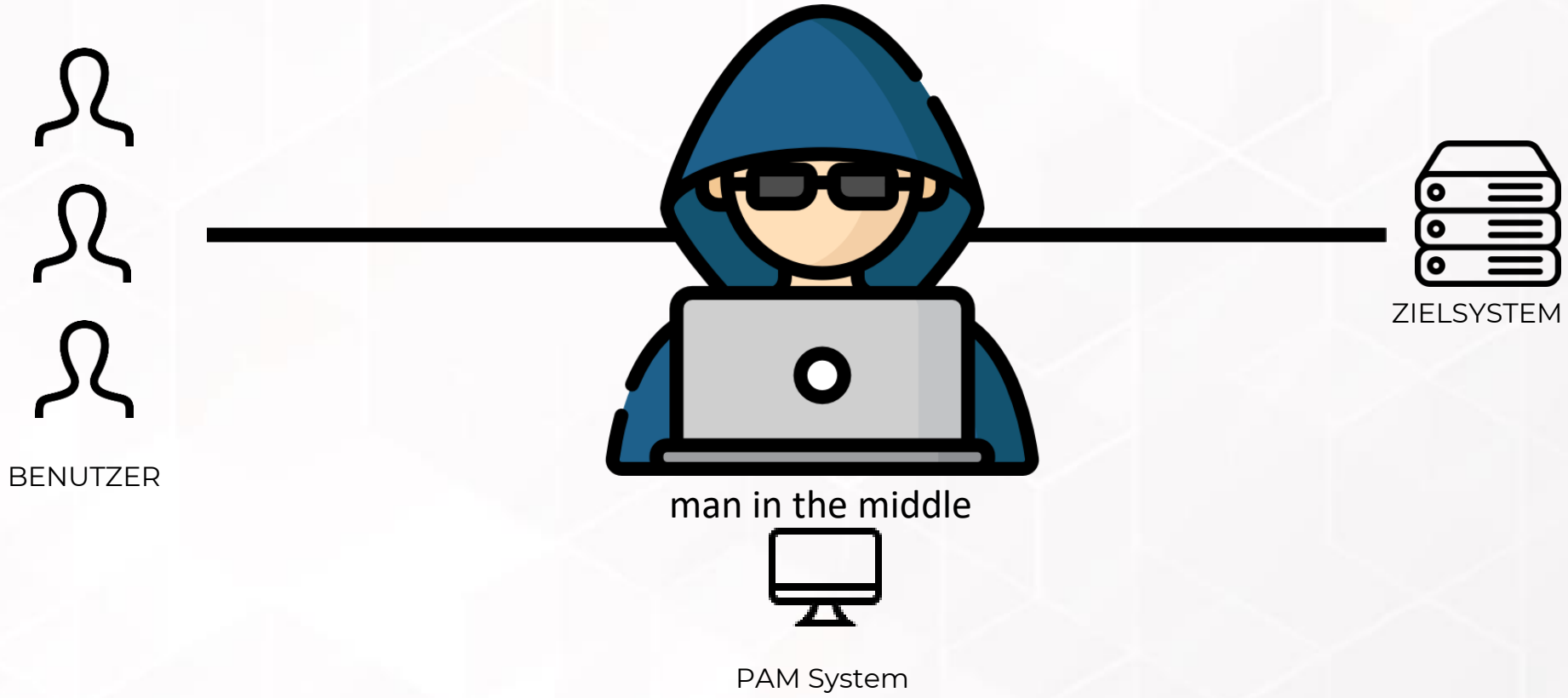
2016 — WHEEL FUDO PAM

FUDO SECURITY

Was macht PAM?

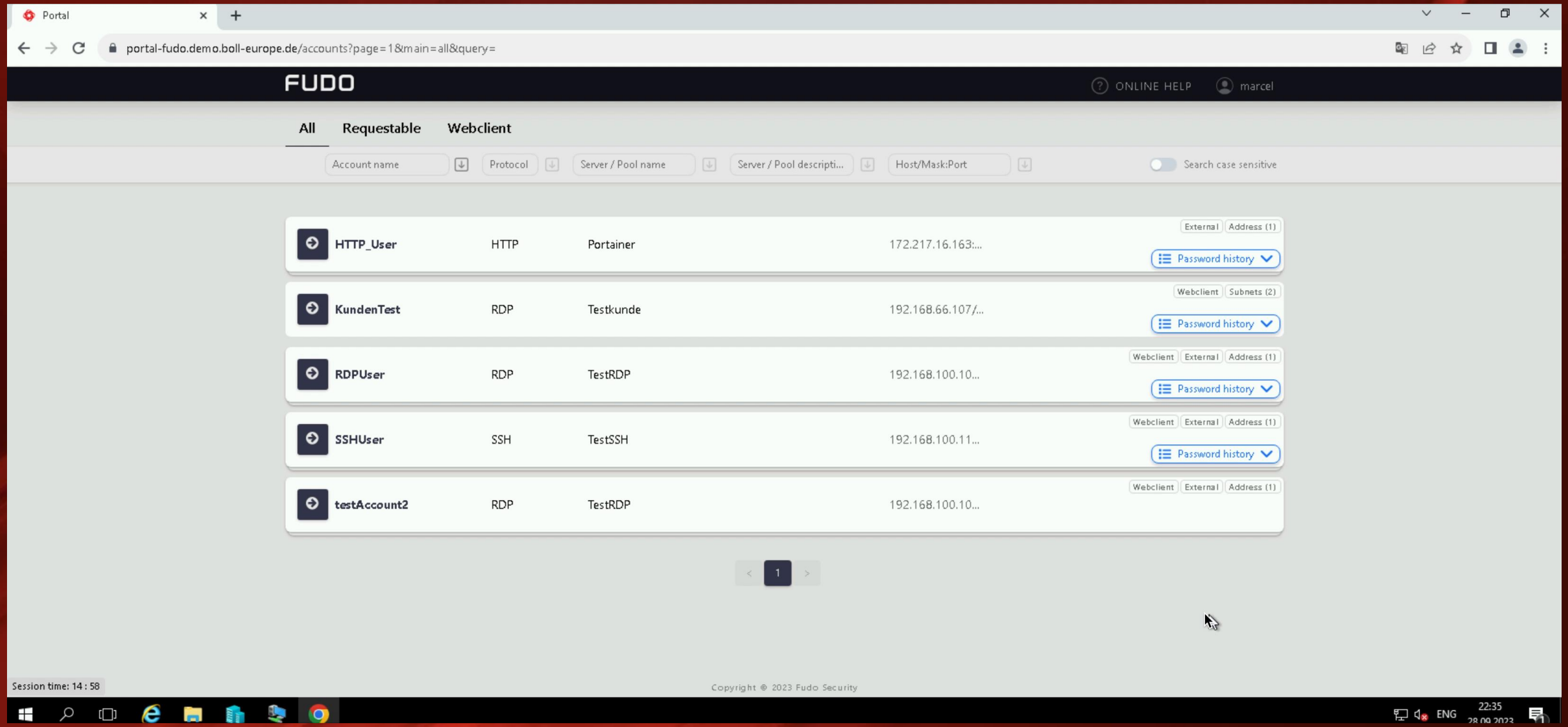
1. Direkter Zugriff auf System nur über PAM möglich
2. Nur berechtigte Mitarbeiter bekommen Zugriff
3. Alle Sessions werden aufgezeichnet
4. Externe Mitarbeiter können beaufsichtigt werden

It´s not a cyber attack, it´s a feature!

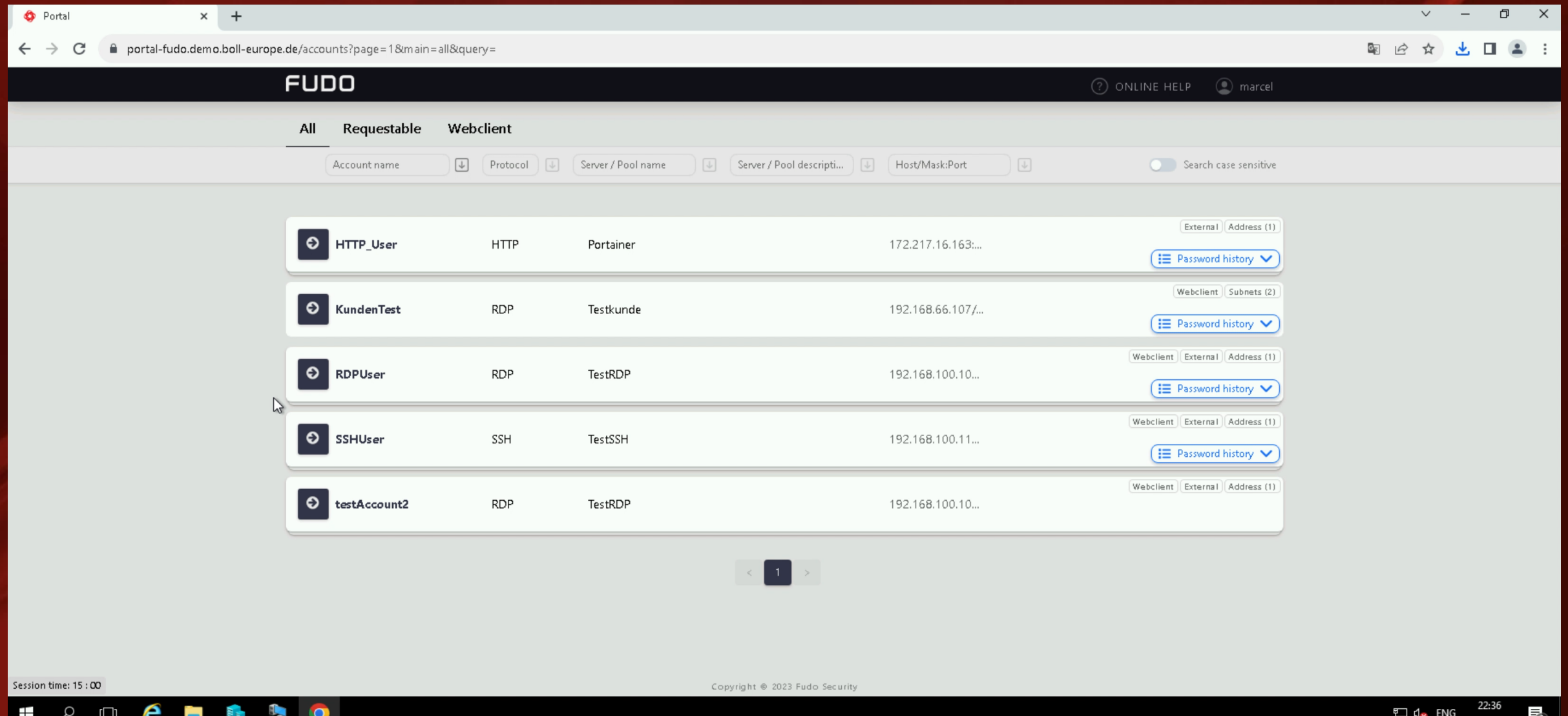


FUDO SECURITY

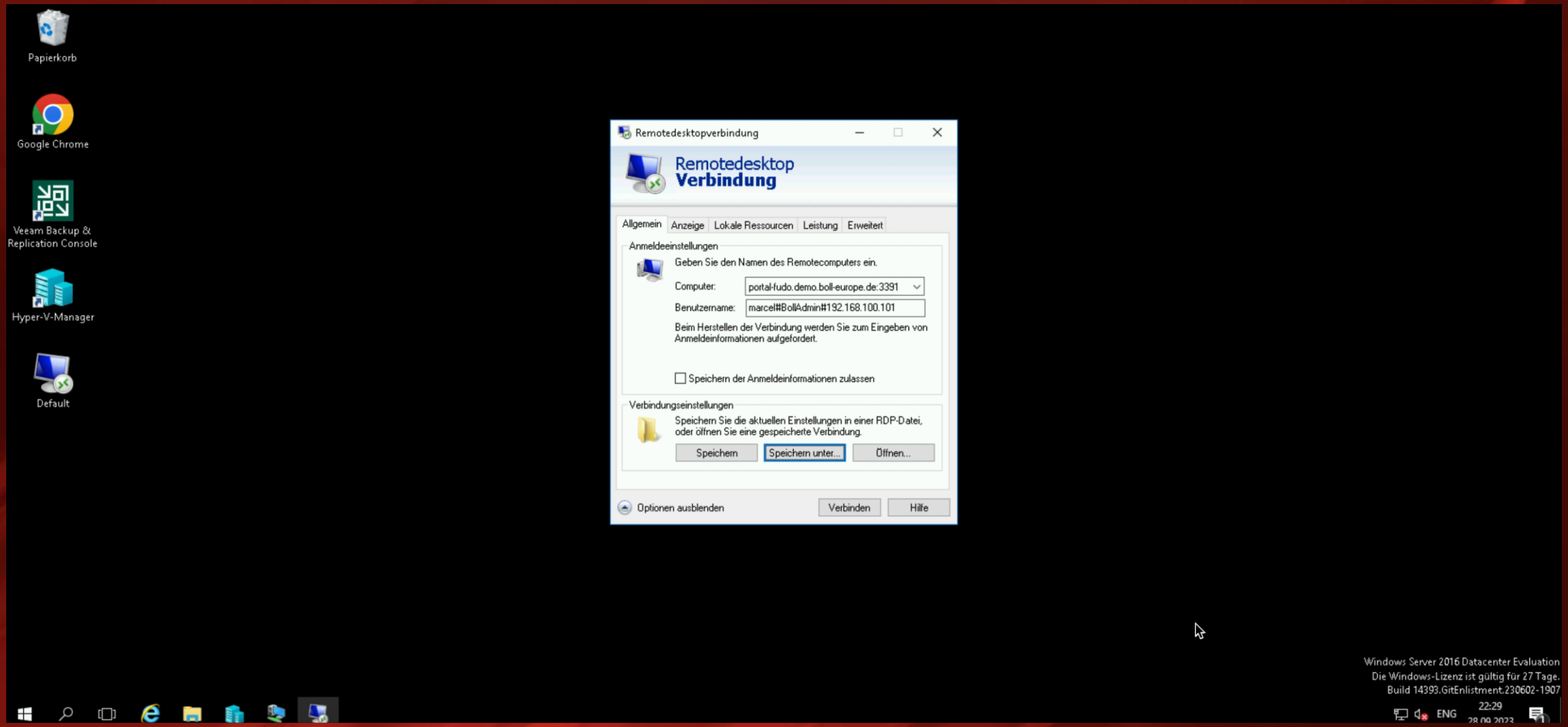
GIF mit Beispiel Verbindung Web



GIF mit Beispiel Verbindung Native

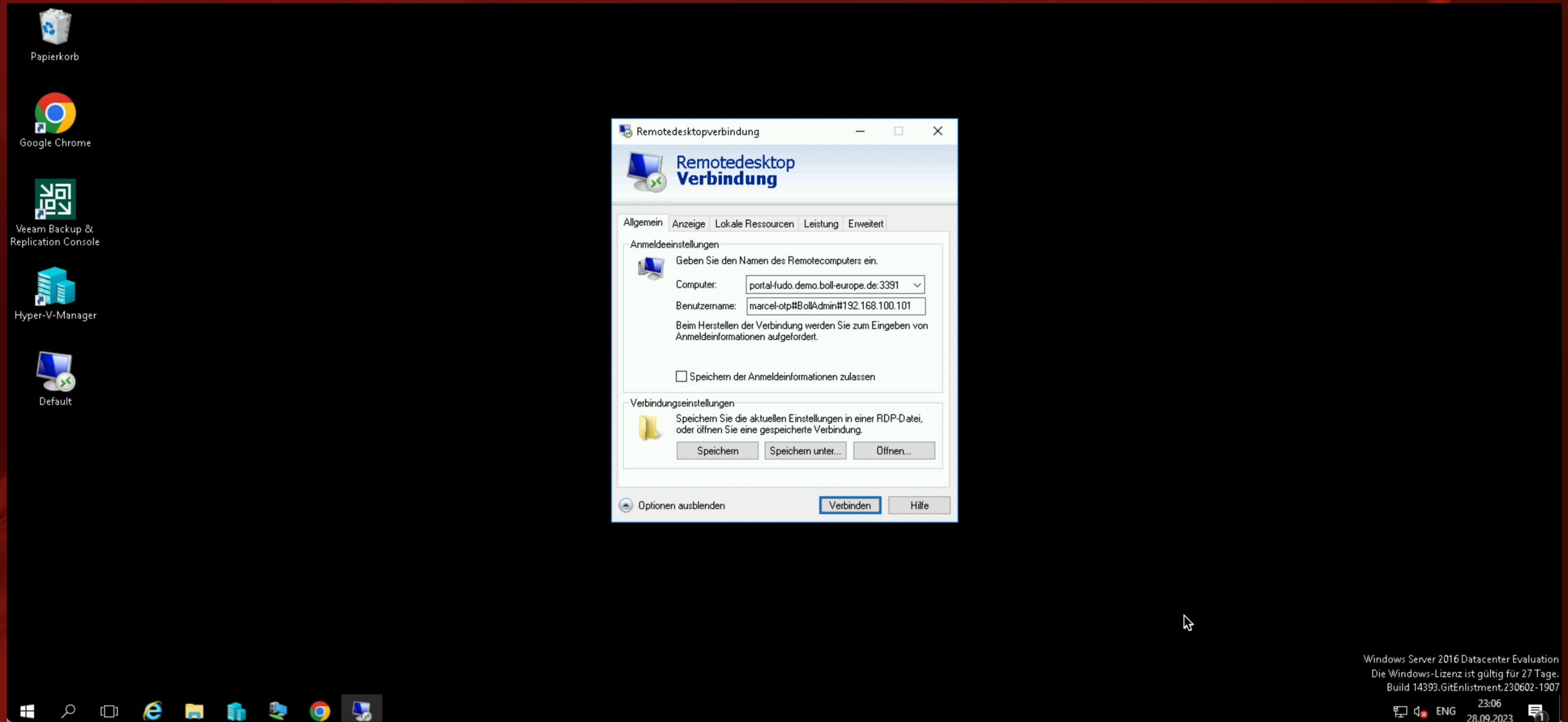


Web? Native bitte!

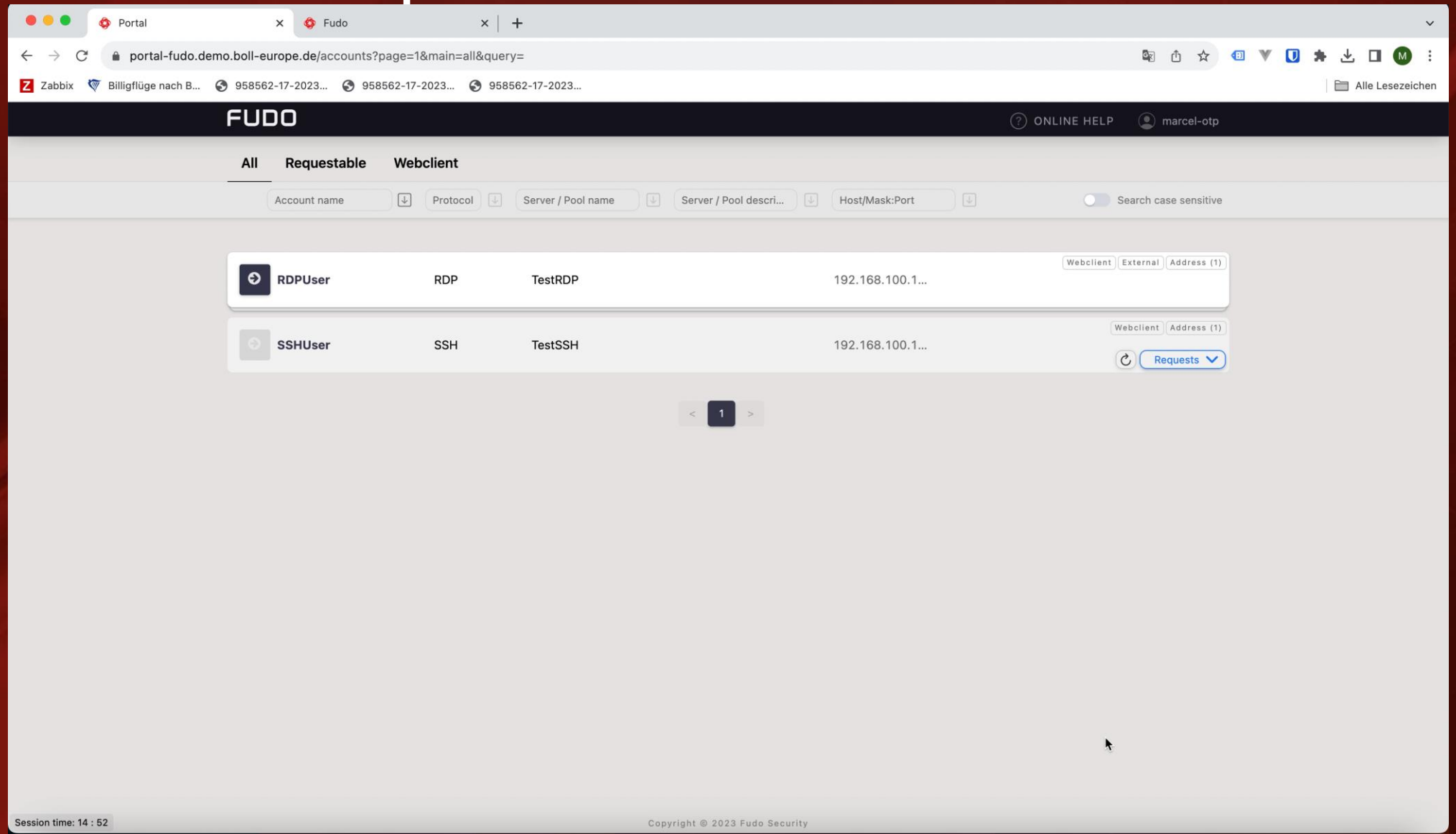


marcel#BollAdmin#192.168.100.101

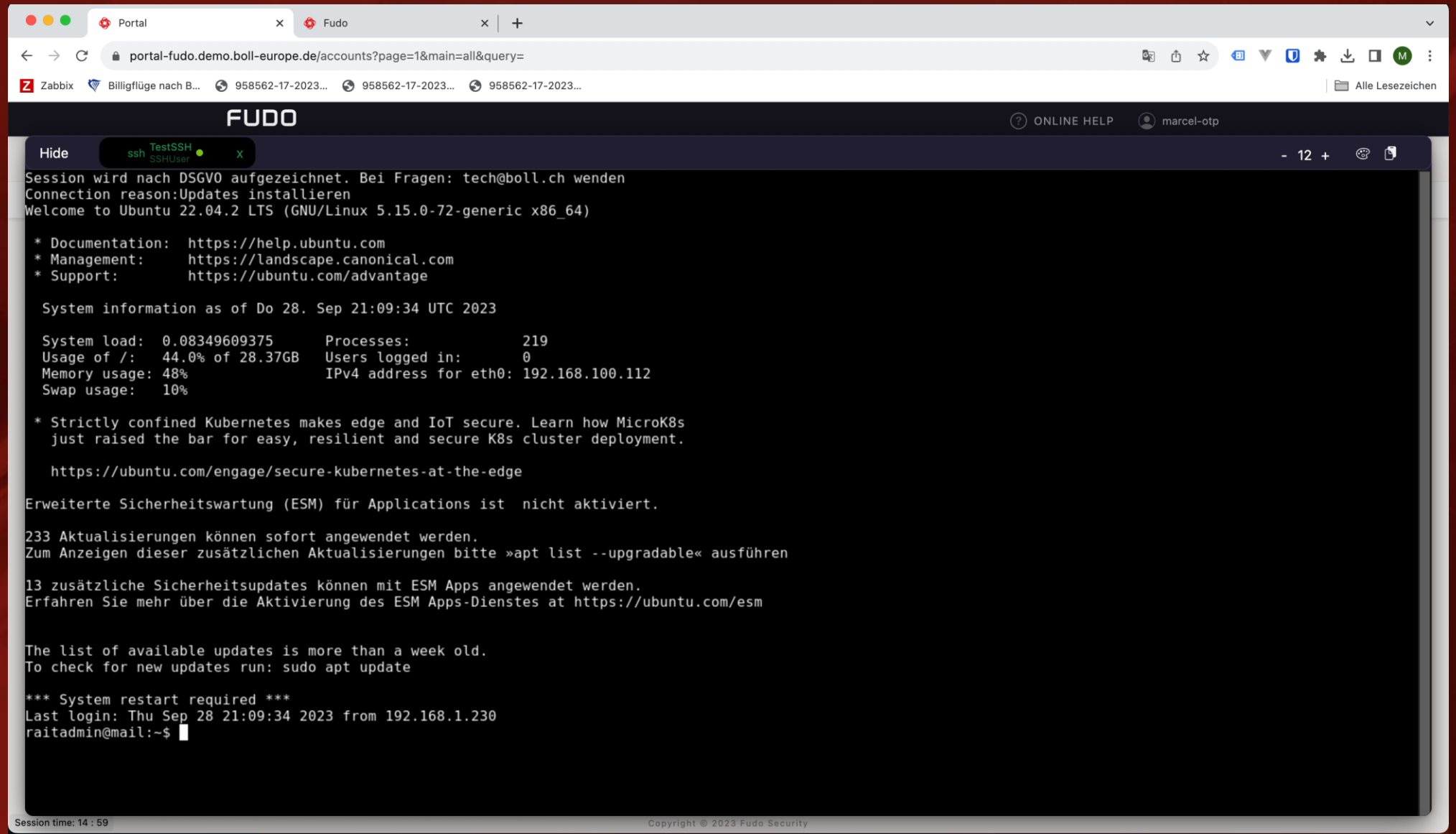
2FA


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
Windows Server 2016 Datacenter Evaluation
Die Windows-Lizenz ist gültig für 27 Tage.
Build 14393.GitEnlistment.230602-1907
ENG
23:06
28.09.2023

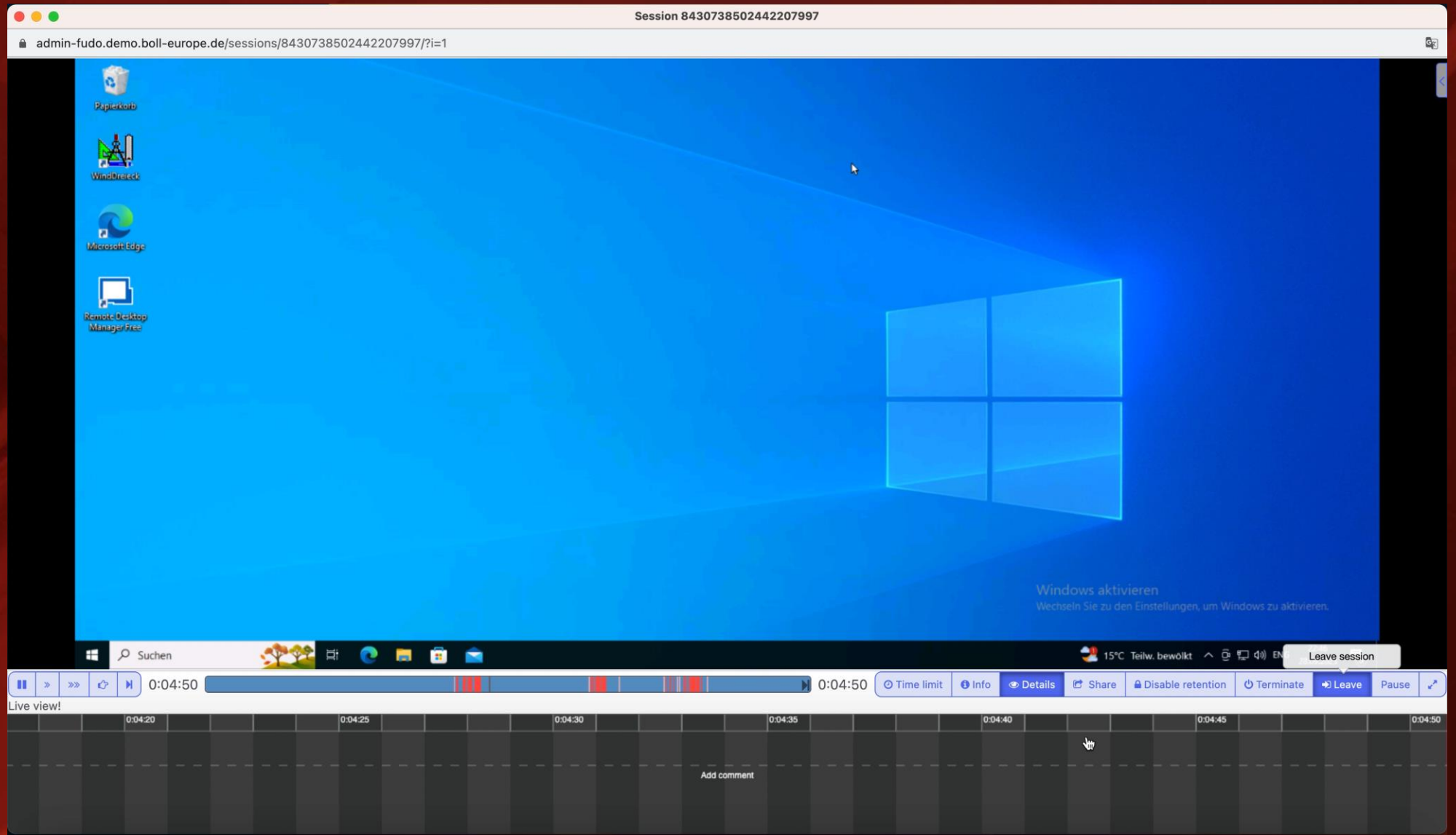
Access Request



Policies


Portal
Fudo
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
Hide
ssh TestSSH SSHUser
- 12 +
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:~$
Session time: 14 : 59
Copyright © 2023 Fudo Security

Einfach nur Video? Nein, Rohdaten!

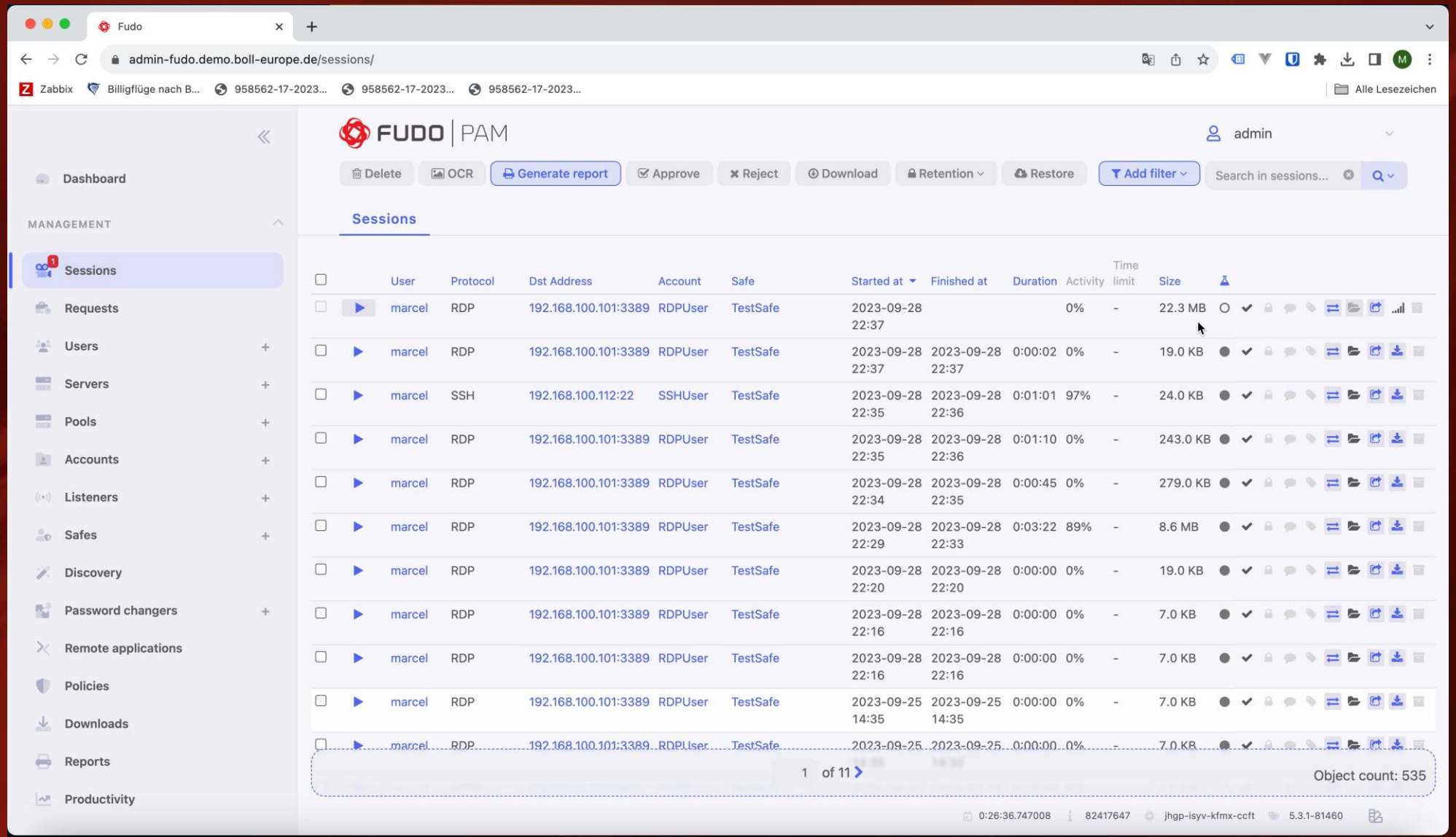


Rohdaten = Viel Speicher?

MP4 1080p 3GB/Stunde (170 Stunden)
RDP 1080p 218MB/Stunde (2348 Stunden)

SSH nur Zeilen!

Warum Fudo? Usability!



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“

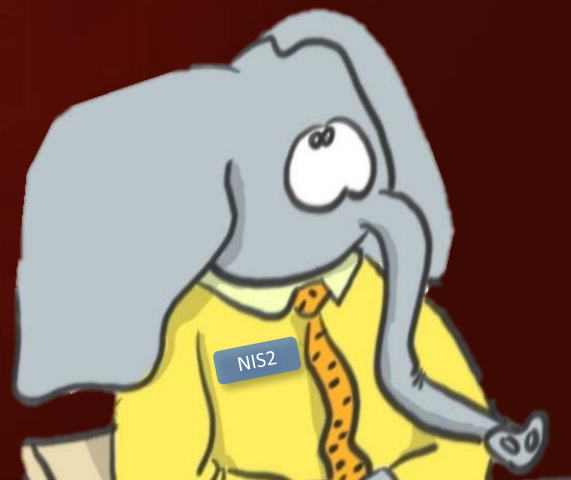
PAM und NIS2?

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!



	F1002	F3002	F5000	Fudo Virtual Machine
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!