FRESCHE SOLUTIONS

IBM i Security Trends for 2025

June 19th, 2025

Housekeeping

- ✉ Slides & session recording will be e-mailed to you
- Ask questions
- Share your thoughts

Presenter Introduction

Pauline Brazil Ayala

Product Manager, Security Products
Fresche Solutions

pauline.ayala@freschesolutions.com

Tony Perera

Sr. Dev Manager, Security Products
Fresche Solutions

tony.perera@freschesolutions.com

Fresche Security Overview

Global provider of security software products & services

Customers include many Fortune 500 and Global 2000 companies, as well as many small to mid-sized IBM i organizations

12+ year track record of success

IBM i Security Partner & Advisory Council Member

Cybercrime & Threats

Top threats include:

- Ransomware
- Exploitation of remote work
- Phishing/Spoofing
- Sophisticated threats using AI

2024 Q4: Highest recorded level of ransomware activity, according to the FBI

Almost nine million DDoS attacks in the second half of 2024, up 12.75%

Nearly 50% of IBM i shops have little to no security knowledge and skills

71% of organizations are not prepared to recover from a ransomware attack

43% of organizations don’t have any cybersecurity plan in place

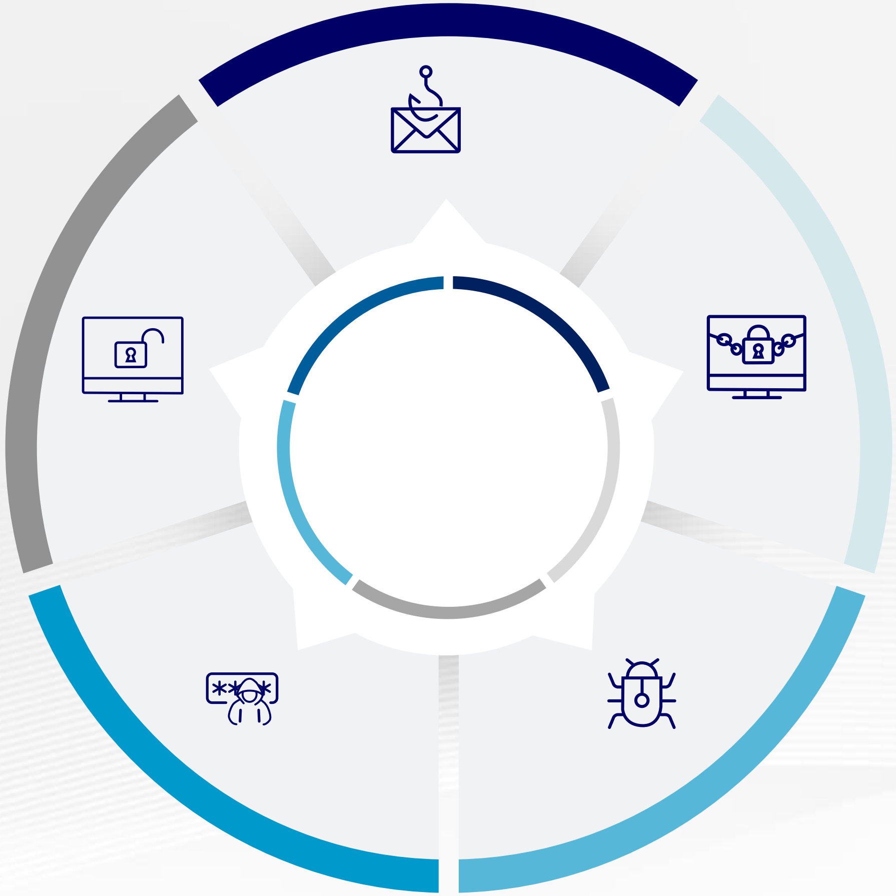
FBI's 2024 report reveals $16.6 Billion in losses, a 33% increase from 2023

87% of firms hit by AI cyberattacks

Sources: Fresche, IBM, Forbes/cybersecurity-in-2025, Secure World

Cybersecurity Threats to IBM i Data

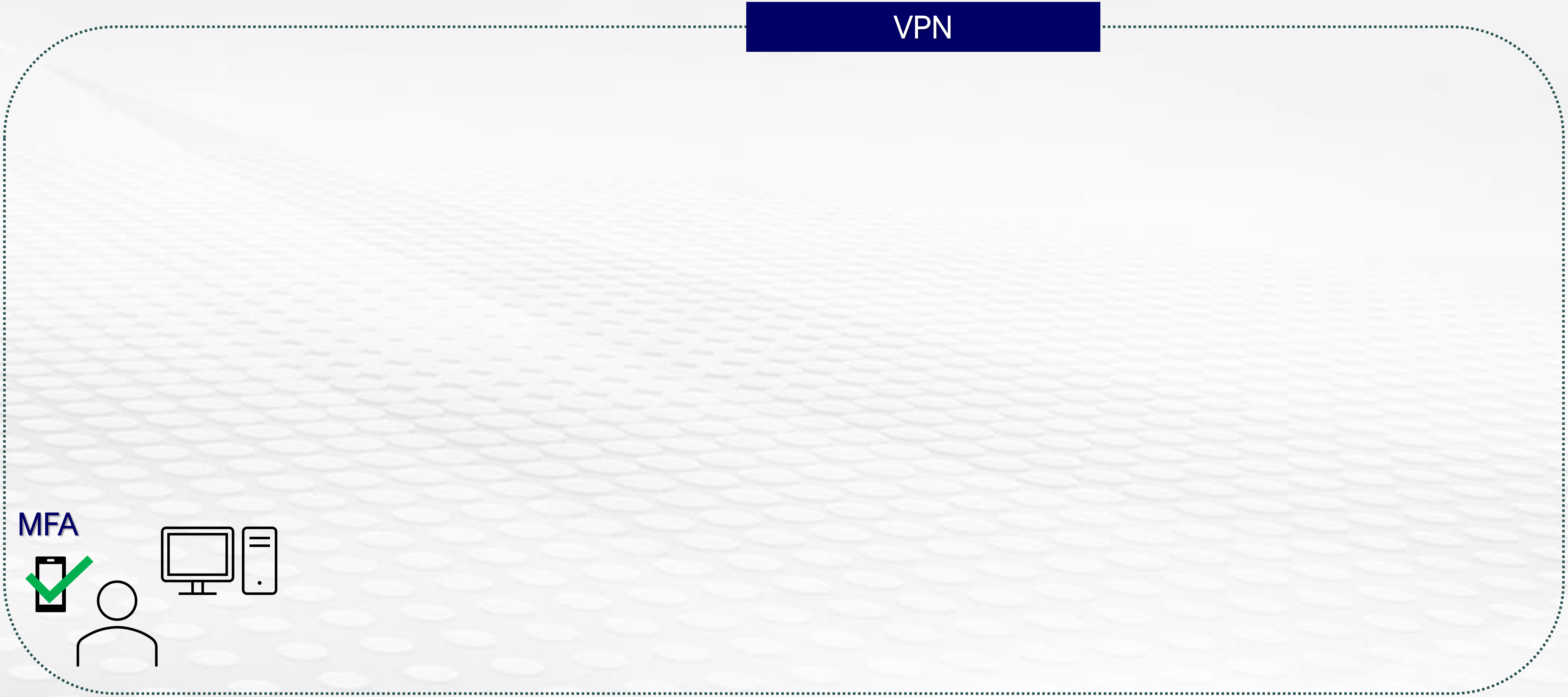
- Phishing
- Ransomware
- Malware
- Credential Hijacking
- Data Breaches



FRESCHE

Phishing Attack

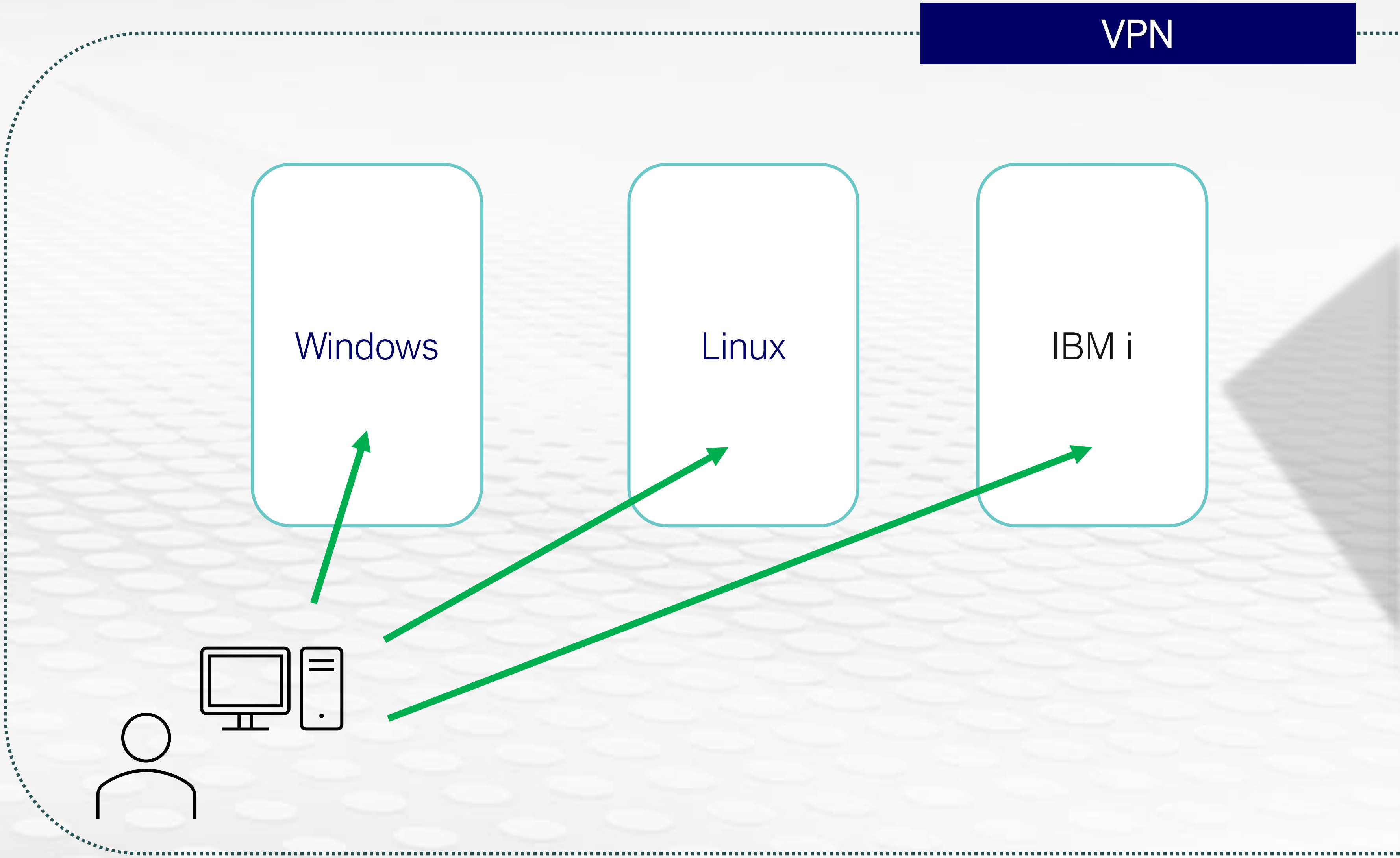
Phishing Attack

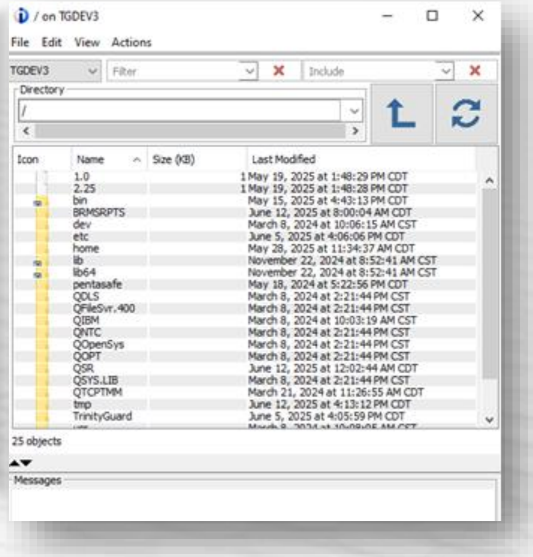


VPN

MFA

Phishing Attack



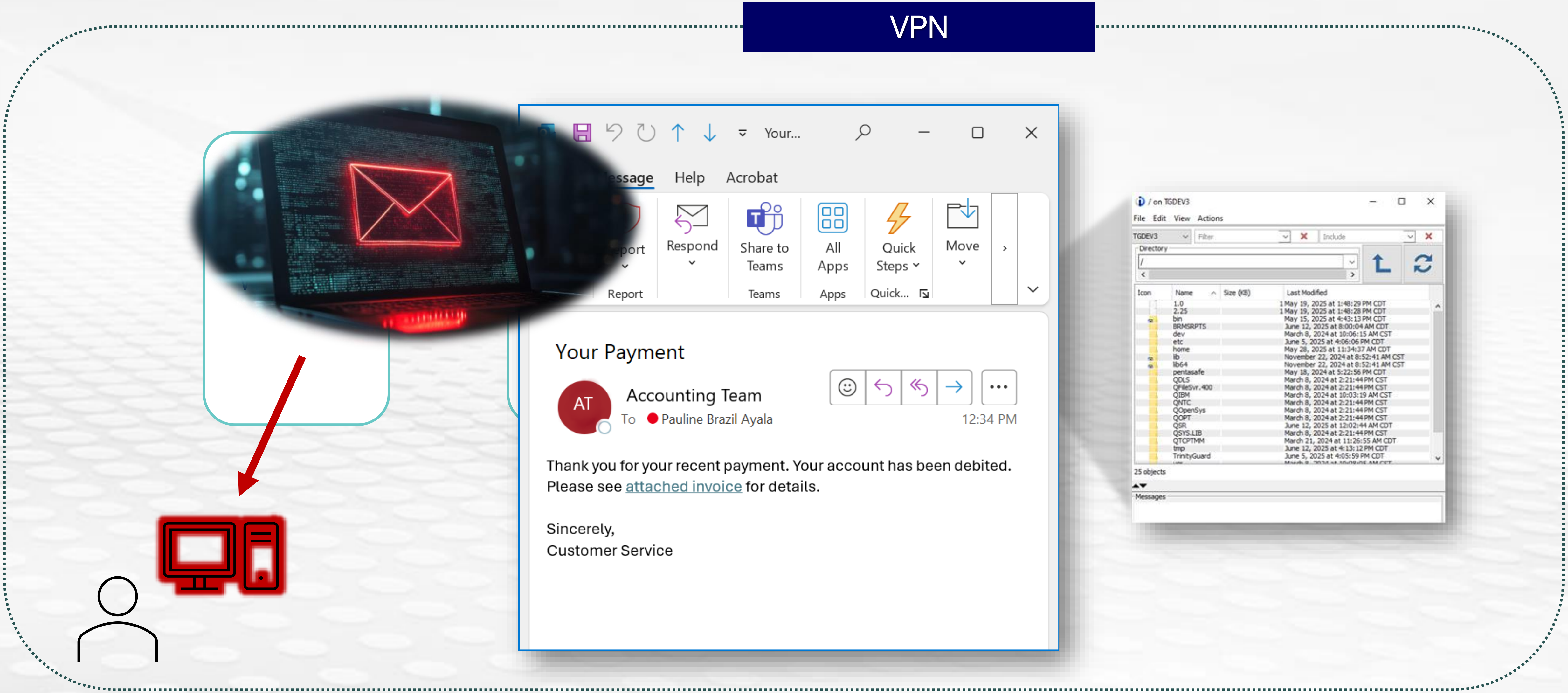


Icon	Name	Size (KB)	Last Modified
	1.0	1	May 19, 2025 at 1:48:29 PM CDT
	2.25	1	May 19, 2025 at 1:48:28 PM CDT
	bin		May 15, 2025 at 4:43:13 PM CDT
	BRMSRPTS		June 12, 2025 at 8:00:04 AM CDT
	dev		March 8, 2024 at 10:06:15 AM CST
	etc		June 5, 2025 at 4:06:06 PM CDT
	home		May 28, 2025 at 11:34:37 AM CDT
	lib		November 22, 2024 at 8:52:41 AM CST
	lib64		November 22, 2024 at 8:52:41 AM CST
	pentasafe		May 18, 2024 at 5:22:56 PM CDT
	QDLS		March 8, 2024 at 2:21:44 PM CST
	QFileSvr.400		March 8, 2024 at 2:21:44 PM CST
	QIBM		March 8, 2024 at 10:03:19 AM CST
	QNTC		March 8, 2024 at 2:21:44 PM CST
	QOpenSys		March 8, 2024 at 2:21:44 PM CST
	QOPT		March 8, 2024 at 2:21:44 PM CST
	QSR		June 12, 2025 at 12:02:44 AM CDT
	QSYS.LIB		March 8, 2024 at 2:21:44 PM CST
	QTCPTMM		March 21, 2024 at 11:26:55 AM CDT
	tmp		June 12, 2025 at 4:13:12 PM CDT
	TrinityGuard		June 5, 2025 at 4:05:59 PM CDT

25 objects

Messages

Phishing Attack



Your Payment

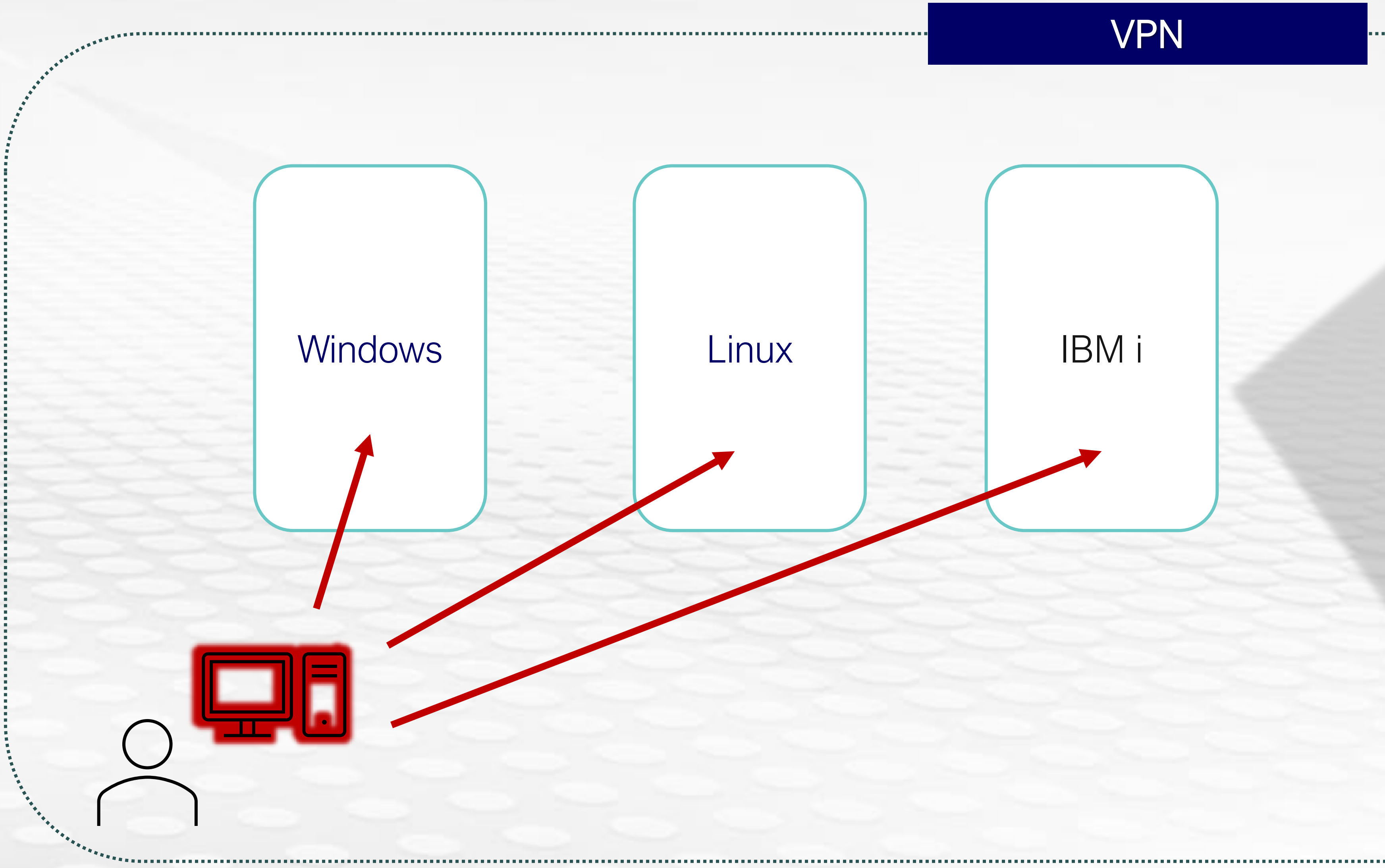
Accounting Team
To Pauline Brazil Ayala
12:34 PM

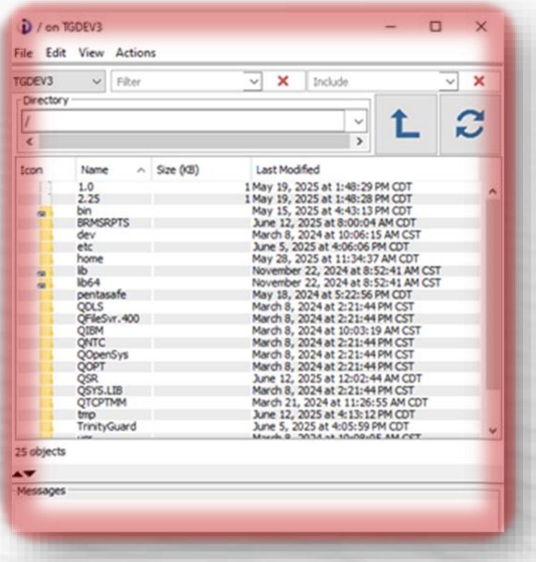
Thank you for your recent payment. Your account has been debited. Please see attached invoice for details.

Sincerely,
Customer Service

Icon	Name	Size (KB)	Last Modified
	1.0	1	May 19, 2025 at 1:48:29 PM CDT
	2.25	1	May 19, 2025 at 1:48:28 PM CDT
	bin		May 15, 2025 at 4:43:13 PM CDT
	BRMSRPTS		June 12, 2025 at 8:00:04 AM CDT
	dev		March 8, 2024 at 10:06:15 AM CST
	etc		June 5, 2025 at 4:06:06 PM CDT
	home		May 28, 2025 at 11:34:37 AM CDT
	lib		November 22, 2024 at 8:52:41 AM CST
	lib64		November 22, 2024 at 8:52:41 AM CST
	pentasafe		May 18, 2024 at 5:22:56 PM CDT
	QDLS		March 8, 2024 at 2:21:44 PM CST
	QFileSvr.400		March 8, 2024 at 2:21:44 PM CST
	QIBM		March 8, 2024 at 10:03:19 AM CST
	QNTC		March 8, 2024 at 2:21:44 PM CST
	QOpenSys		March 8, 2024 at 2:21:44 PM CST
	QOPT		March 8, 2024 at 2:21:44 PM CST
	QSR		June 12, 2025 at 12:02:44 AM CDT
	QSYS.LIB		March 8, 2024 at 2:21:44 PM CST
	QTCPTMM		March 21, 2024 at 11:26:55 AM CDT
	tmp		June 12, 2025 at 4:13:12 PM CDT
	TrinityGuard		June 5, 2025 at 4:05:59 PM CDT

Phishing Attack



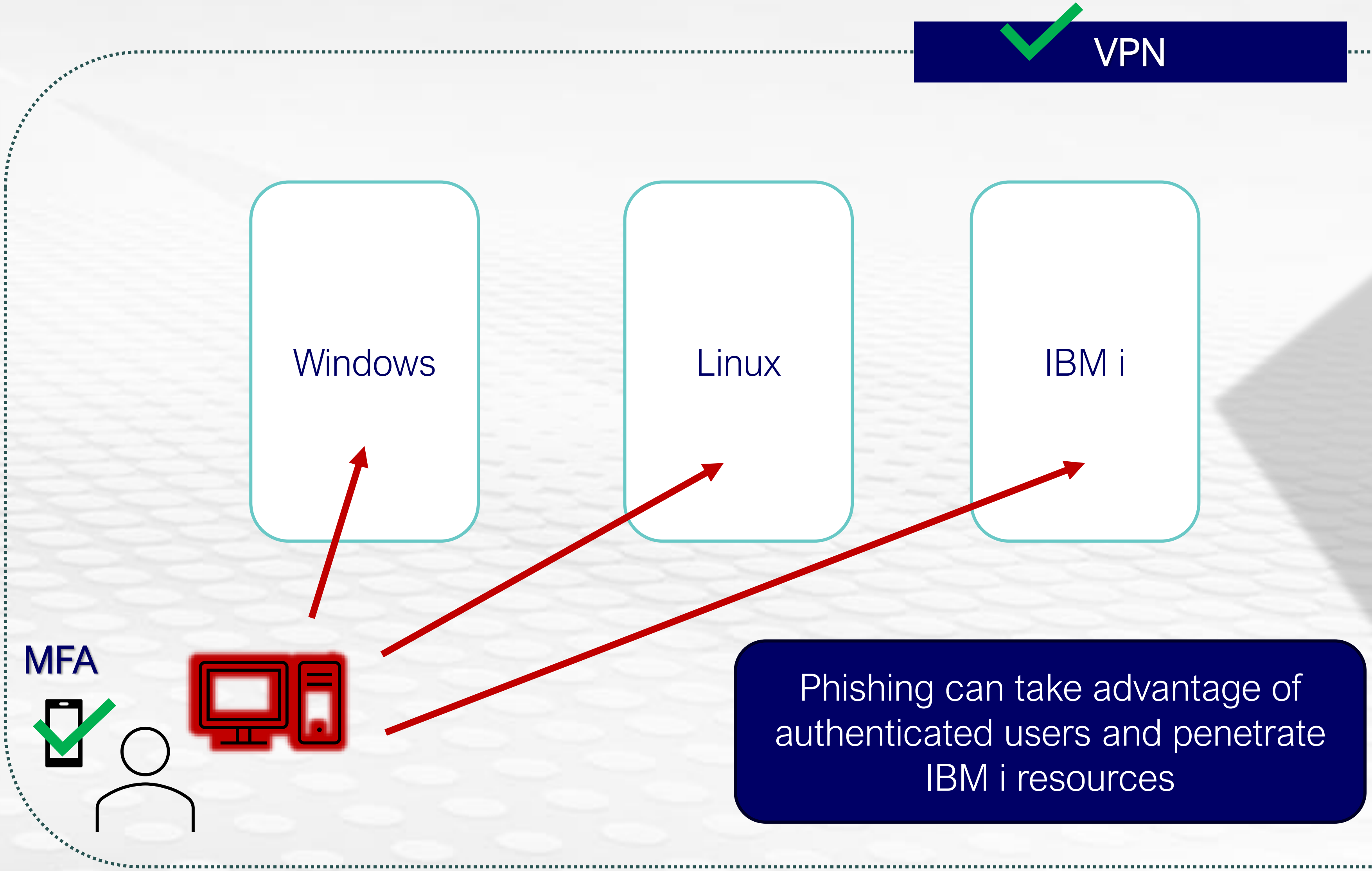


Icon	Name	Size (KB)	Last Modified
	1.0	1	May 19, 2025 at 1:48:29 PM CDT
	2.25	1	May 19, 2025 at 1:48:28 PM CDT
	bin		May 15, 2025 at 4:43:13 PM CDT
	BRMSRPTS		June 12, 2025 at 8:00:04 AM CDT
	dev		March 8, 2024 at 10:06:15 AM CST
	etc		June 5, 2025 at 4:06:06 PM CDT
	home		May 28, 2025 at 11:34:37 AM CDT
	lib		November 22, 2024 at 8:52:41 AM CST
	lib64		November 22, 2024 at 8:52:41 AM CST
	pentasafe		May 18, 2024 at 5:22:56 PM CDT
	QDLS		March 8, 2024 at 2:21:44 PM CST
	QFileSvr.400		March 8, 2024 at 2:21:44 PM CST
	QIBM		March 8, 2024 at 10:03:19 AM CST
	QNTC		March 8, 2024 at 2:21:44 PM CST
	QOpenSys		March 8, 2024 at 2:21:44 PM CST
	QOPT		March 8, 2024 at 2:21:44 PM CST
	QSR		June 12, 2025 at 12:02:44 AM CDT
	QSYS.LIB		March 8, 2024 at 2:21:44 PM CST
	QTCPTMM		March 21, 2024 at 11:26:55 AM CDT
	tmp		June 12, 2025 at 4:13:12 PM CDT
	TrinityGuard		June 5, 2025 at 4:05:59 PM CDT

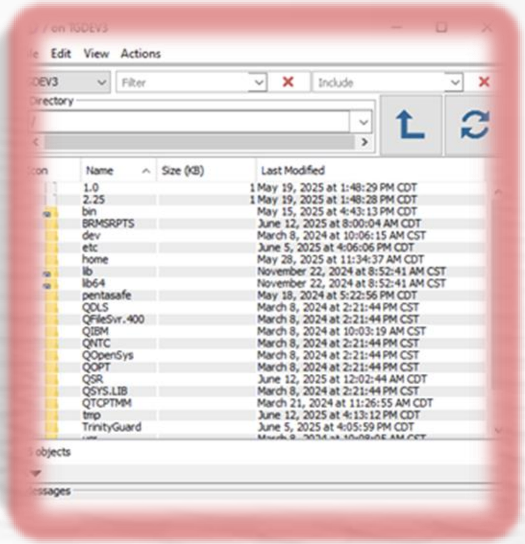
25 objects

Messages

Phishing Attack



Phishing can take advantage of authenticated users and penetrate IBM i resources

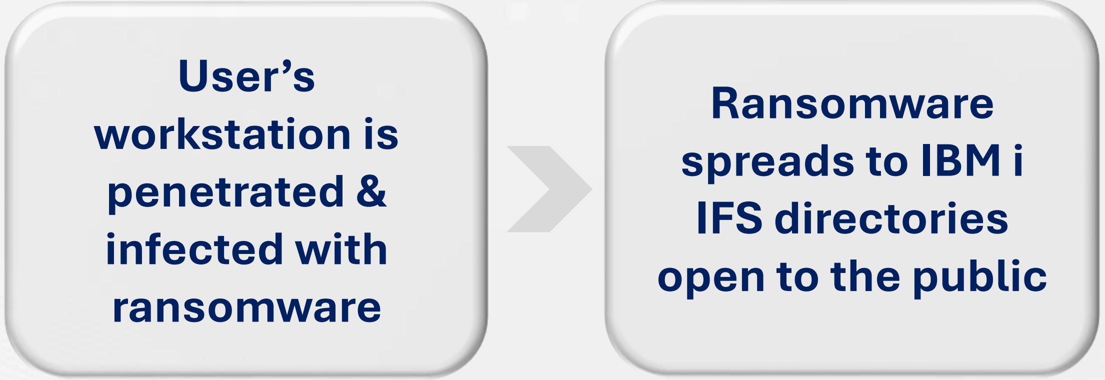


Name	Size (KB)	Last Modified
1.0	1	May 19, 2025 at 1:48:29 PM CDT
2.25	1	May 19, 2025 at 1:48:28 PM CDT
bin		May 15, 2025 at 4:43:13 PM CDT
BRMSRPTS		June 12, 2025 at 8:00:04 AM CDT
dev		March 8, 2024 at 10:06:15 AM CST
etc		June 5, 2025 at 4:06:06 PM CDT
home		May 28, 2025 at 11:34:37 AM CDT
lib		November 22, 2024 at 8:52:41 AM CST
lib64		November 22, 2024 at 8:52:41 AM CST
pentasafe		May 18, 2024 at 5:22:56 PM CDT
QDLS		March 8, 2024 at 2:21:44 PM CST
QFileSvr.400		March 8, 2024 at 2:21:44 PM CST
QIBM		March 8, 2024 at 10:03:19 AM CST
QNTC		March 8, 2024 at 2:21:44 PM CST
QOpenSys		March 8, 2024 at 2:21:44 PM CST
QOPT		March 8, 2024 at 2:21:44 PM CST
QSR		June 12, 2025 at 12:02:44 AM CDT
QSYS.LIB		March 8, 2024 at 2:21:44 PM CST
QTCPTMM		March 21, 2024 at 11:26:55 AM CDT
tmp		June 12, 2025 at 4:13:12 PM CDT
TrinityGuard		June 5, 2025 at 4:05:59 PM CDT

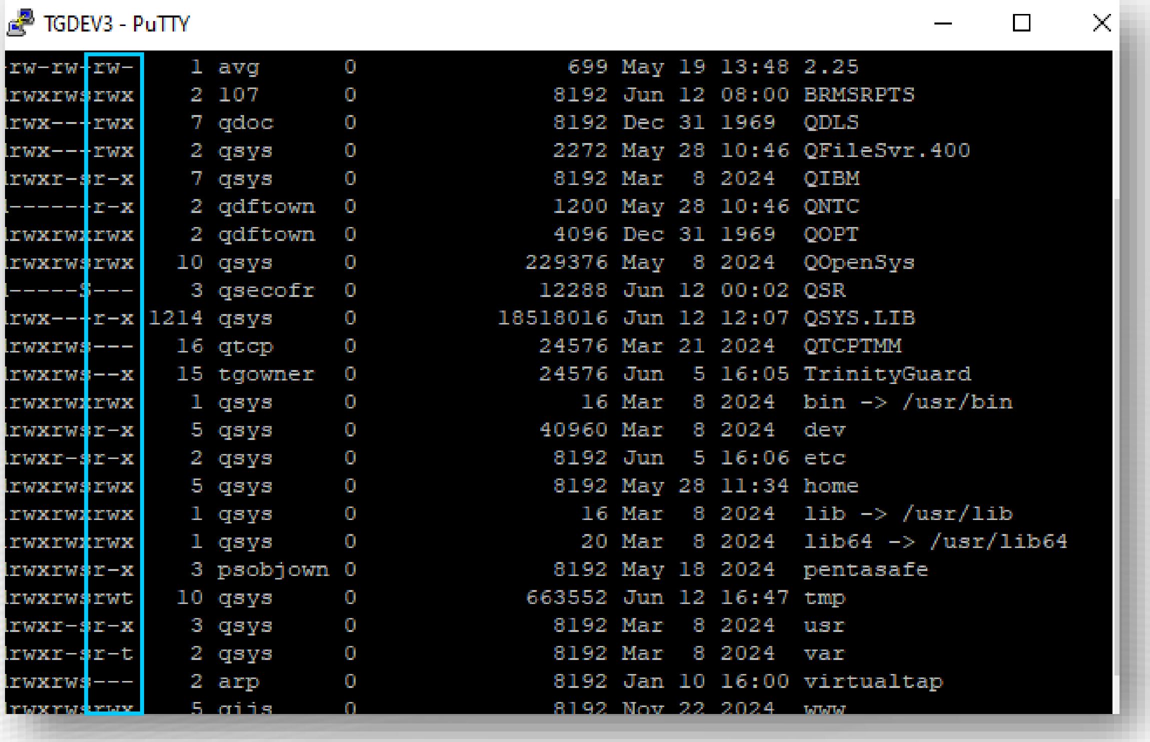
Ransomware Attack

Ransomware Attack

Scenario


User's workstation is penetrated & infected with ransomware

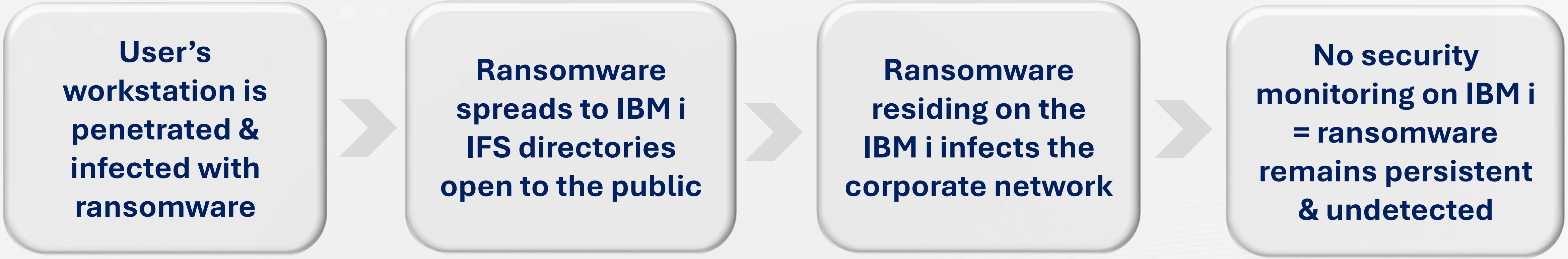
Ransomware spreads to IBM i IFS directories open to the public



```
-rw-rw-rw-    1 avg       0             699 May 19 13:48 2.25
drwxrwsrwx    2 107       0            8192 Jun 12 08:00 BRMSRPTS
drwx---rwx    7 qdoc      0            8192 Dec 31 1969  QDLS
drwx---rwx    2 qsys      0            2272 May 28 10:46 QFileSvr.400
drwxr-sr-x    7 qsys      0            8192 Mar  8 2024  QIBM
d------r-x    2 qdftown   0            1200 May 28 10:46 QNTC
drwxrwxrwx    2 qdftown   0            4096 Dec 31 1969  QOPT
drwxrwsrwx   10 qsys      0          229376 May  8 2024  QOpenSys
d-----S---    3 qsecofr   0           12288 Jun 12 00:02 QSR
drwx---r-x 1214 qsys      0        18518016 Jun 12 12:07 QSYS.LIB
drwxrws---   16 qtcp      0           24576 Mar 21 2024  QTCPTMM
drwxrws--x   15 tgowner   0           24576 Jun  5 16:05 TrinityGuard
lrwxrwxrwx    1 qsys      0              16 Mar  8 2024  bin -> /usr/bin
drwxrwsr-x    5 qsys      0           40960 Mar  8 2024  dev
drwxr-sr-x    2 qsys      0            8192 Jun  5 16:06 etc
drwxrwsrwx    5 qsys      0            8192 May 28 11:34 home
lrwxrwxrwx    1 qsys      0              16 Mar  8 2024  lib -> /usr/lib
lrwxrwxrwx    1 qsys      0              20 Mar  8 2024  lib64 -> /usr/lib64
drwxrwsr-x    3 psobjown  0            8192 May 18 2024  pentasafe
drwxrwsrwt   10 qsys      0          663552 Jun 12 16:47 tmp
drwxr-sr-x    3 qsys      0            8192 Mar  8 2024  usr
drwxr-sr-t    2 qsys      0            8192 Mar  8 2024  var
drwxrws---    2 arp       0            8192 Jan 10 16:00 virtualtap
drwxrwsrwx    5 qijs      0            8192 Nov 22 2024  www
```

Ransomware Attack

Scenario



User’s workstation is penetrated & infected with ransomware

Ransomware spreads to IBM i IFS directories open to the public

Ransomware residing on the IBM i infects the corporate network

No security monitoring on IBM i = ransomware remains persistent & undetected

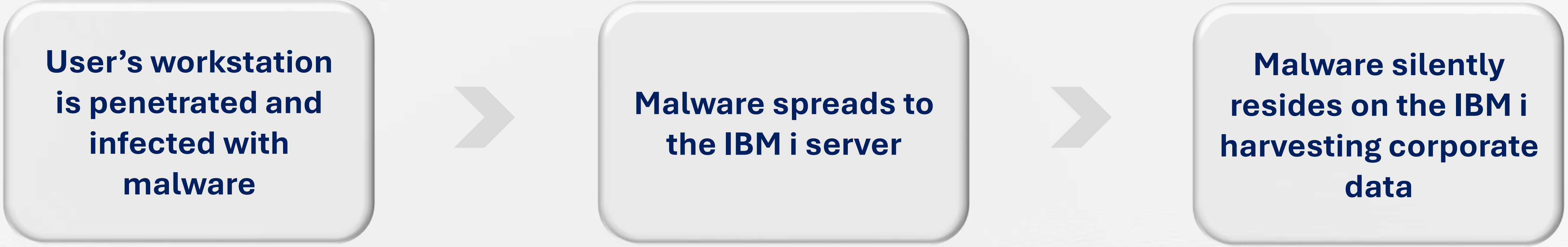
Key Takeaways

- Ransomware will find your weakest servers
- Leaving IBM i servers unprotected can jeopardize all your corporate assets – both IBM i and non-IBM i servers

Malware Harvesting in the IFS

Malware Harvesting in the IFS

Scenario



User's workstation is penetrated and infected with malware

Malware spreads to the IBM i server

Malware silently resides on the IBM i harvesting corporate data

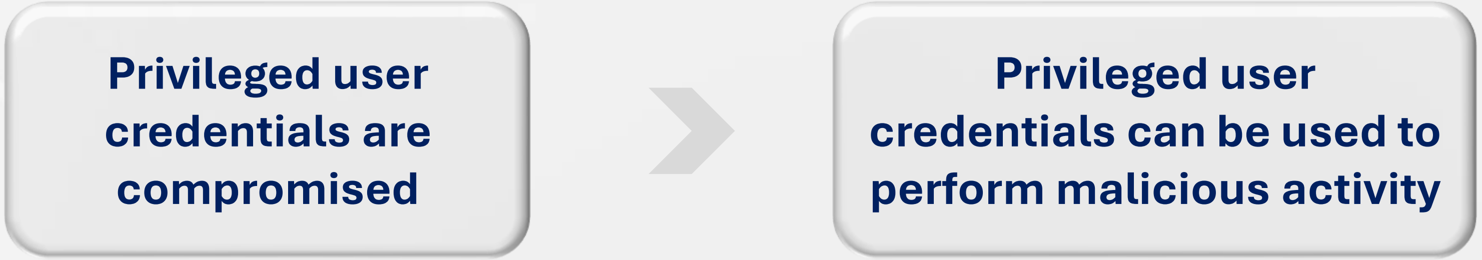
Key Takeaways

- Protecting ALL corporate servers is critical.

Hijacking of Privileged User Accounts

Hijacking of Privileged User Accounts

Scenario



Privileged user credentials are compromised

Privileged user credentials can be used to perform malicious activity

Note: A lot of IBM i servers use 10-byte single case passwords

Key Takeaways

- Make sure all user credentials on all corporate servers adhere to current corporate password policies

Risks & Consequences of Data Breaches

Risks & Consequences of Data Breaches

Data Breaches can occur in any of the previously described scenarios causing...

Corporate data appearing in the dark web

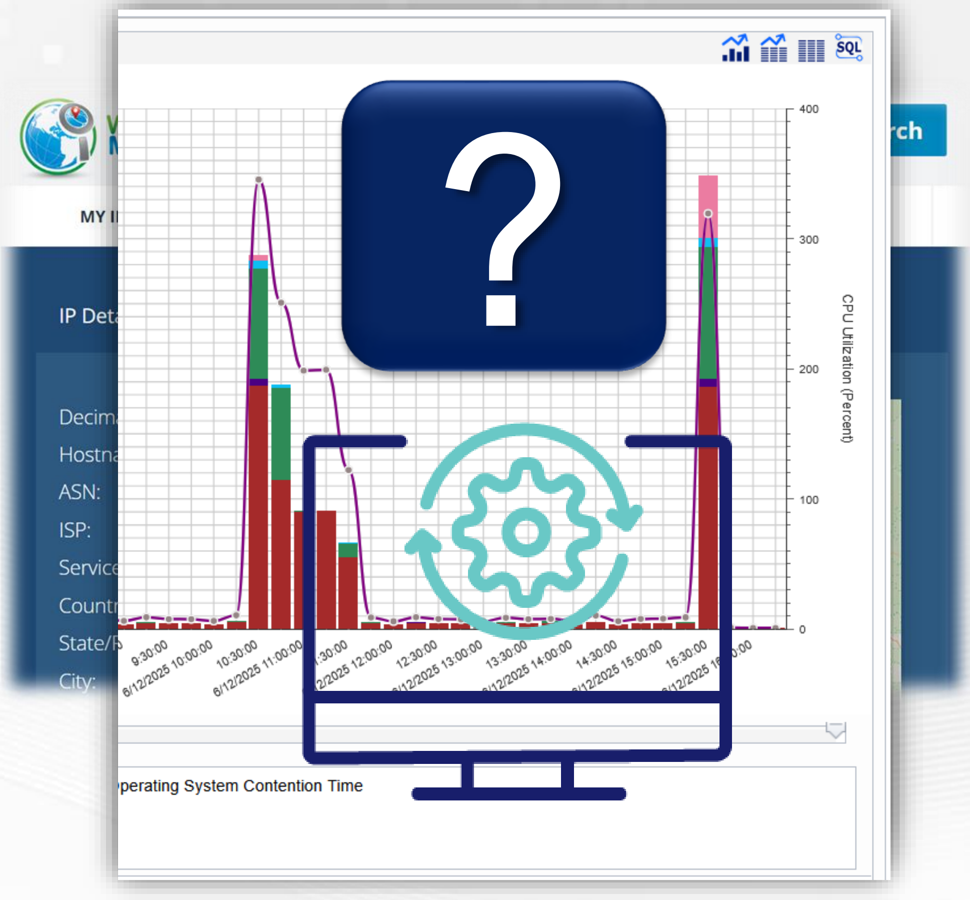
Encryption, Extortion, Fines, Loss of Revenue

Corporate/personal reputation damage

Key Takeaways

- Protect all sensitive data.
- Monitor activity on all servers, including IBM i. (You might already have enterprise monitoring software for your other servers, but not IBM i.)
- Data breaches can be in progress and remain undetected unless you are monitoring your servers.

Symptoms



Strange files in the IFS

Connections from unknown IP addresses

Unreadable data

High CPU consumption

Unknown jobs running

How to Prevent Attacks

Network Security

- Monitor internal and external network traffic to IBM i
- Lock down unauthorized access

Implement Zero Trust

Least Privilege Model

- Users
- IFS Authorities

Activity Monitoring

- Users
- System

Detect Anomolies

- Alert on system security events
- Escalate critical events
- Remediate problems

Next Steps...

Still have questions?
Let us know.

Want to uncover vulnerabilities in your IBM i environment?
We have a Free Trial/POC available.

Get in touch:
Tony.Perera@freschesolutions.com
Pauline.Ayala@freschesolutions.com

Connect with us to get started

IBM i Security

FRESCHE

IBM i Security Trends for 2025

Connect with us

freschesolutions.com

info@freschesolutions.com

@freschesolution

@fresche-solutions