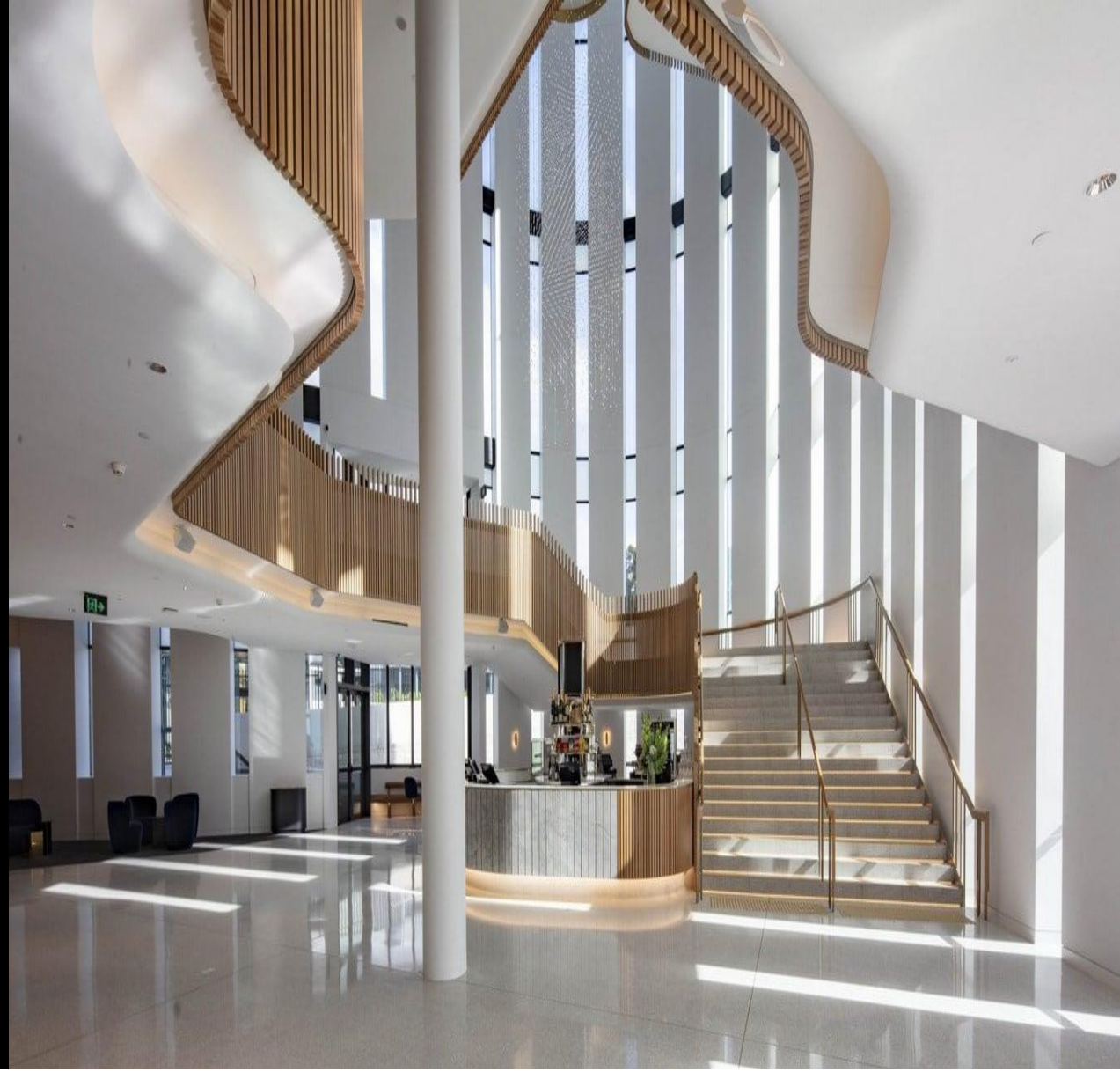
PII & PCI DATA REPORT ASSESSMENT

Assessment Period: 23/10/2025 – 01/12/2025



Assessment Scope

4

Duration (Weeks)

3

Data Sources (Scanned)

7 x Mailboxes

3 x Sites

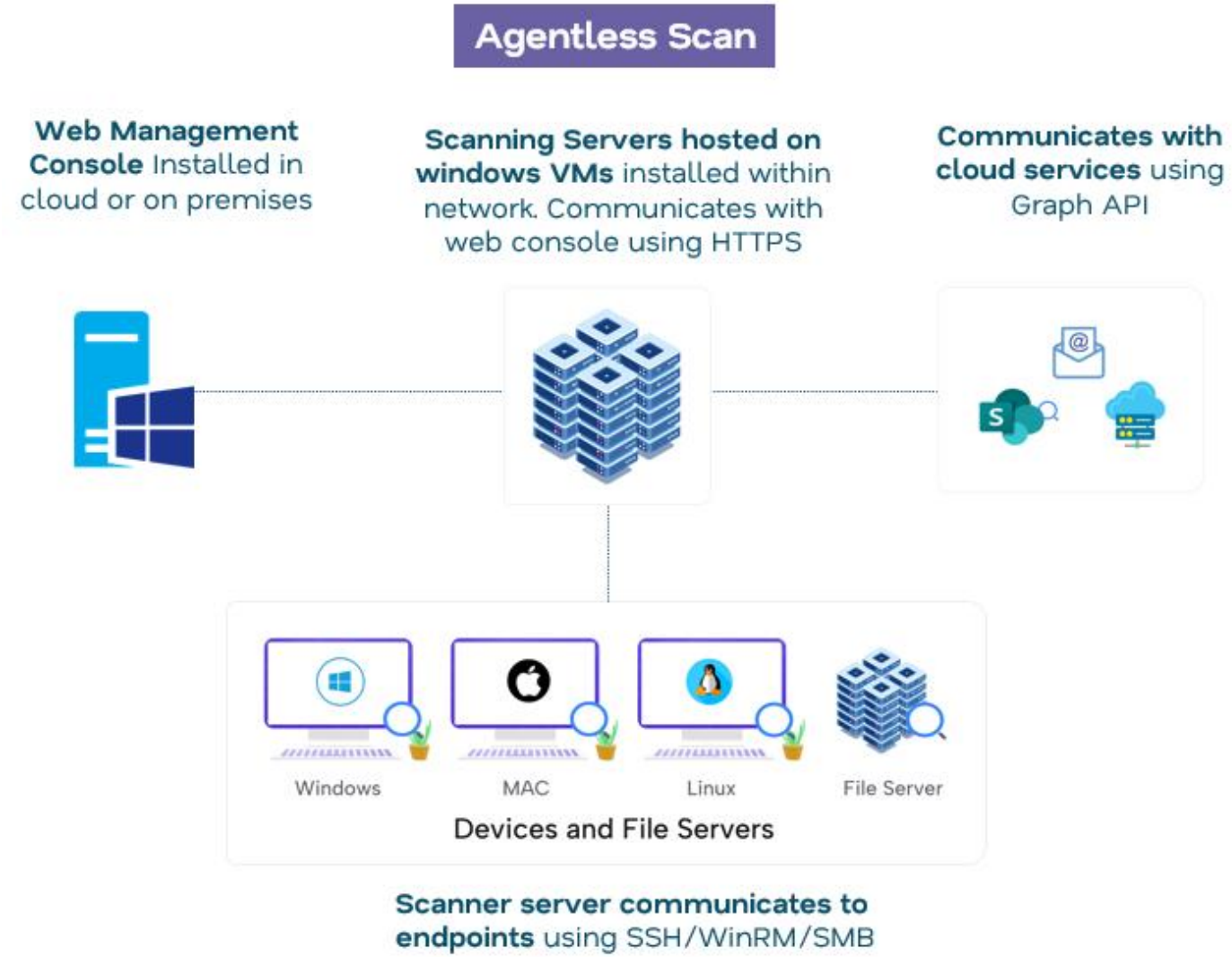
1 x Network Share

9

Data Types (Scanned)

- Australian Bank Account Number
- Australian Driver's License Number
- Australian Medicare Card Number
- Australian Passport Number
- Australian Superannuation Identifier
- Australian Superannuation Member Number
- Australian Tax File Number (TFN)
- Credit Card Number
- Username/Passwords

How GuardWare DISCOVER works?



Executive Summary

Results by Data Type

				Total Files
Australian Bank Account Number	0	669	12739	**13408**
Australian Driver's License Number	0	0	63	**63**
Australian Medicare Card Number	0	3	1	**4**
Australian Passport Number	0	0	29	**29**
Australian Superannuation Identifier	0	4	1391	**1395**
Australian Superannuation Member Number	0	6	90	**96**
Australian Tax File Number (TFN)	0	4	267	**271**
Credit Card Number	0	6	279	**285**
Username/Passwords	11	23	57	**91**

Key Findings

1. Credit card information is being stored, handled and shared in **unencrypted form.** This is a potential breach under PCI-DSS and the Australian Privacy Act.
2. Username/Passwords found in images, documents and e-mails
3. Files containing Tax File Numbers (TFN).
4. Sensitive PII data stored in plaintext (unencrypted).
5. No visibility where sensitive data lives.

5
Top Incidents

High
Overall Risk Posture

589,280
Total Files Scanned

What is the Australian Data Privacy Act?

- It applies to any organisation handling client or customer personal information.
- Monitoring insider activity is essentials because most privacy incidents stem from everyday behaviours such as improper storage, sharing or handling of sensitive data.
- Non-compliance may result in civil penalties, investigations by OAIC and mandatory notifications.

Framework Overview:

Australian Privacy Act

Federal law and mandatory for organisations handling client data

Australian Privacy Principles (APPs)

Practical obligations inside the Act especially APP 11

Notifiable Data Breaches (NDB) Scheme

Mandatory reporting obligations for organisations if they cause or detect a breach involving personal info

Reference: Australian Privacy Act (APP 11)

Mapping Findings to the Australian Privacy Act

	Finding	Obligation	What this means?	Financial Exposure	Result
1	**Credit card information is being stored, handled and shared in unencrypted form.**	APP 3: Collection / APP 11: Security / NBD Scheme	Although the business is not a formal PCI-DSS merchant, the presence of full credit card details (including CCV) places the organisation in accidental PCI scope and creates a significant financial-risk exposure.	Between $130k and $850k and driven by forensic investigation, mandatory notification, compensation and reputational damage.	**Detected**
2	**Username/Passwords found in images, documents and e-mails**	APP 11: Security	Weak passwords storage is considered insufficient security measures under the Act. Must remediate immediately.	Potential ransom extortion: $250k - $5M Business downtime: $50k - $500k / day	**Detected**
3	**Files containing Tax File Numbers (TFN)**	Privacy Act: TFN Rule 2015	Organisations must store, secure and destroy TFN information carefully. Improper storage is a breach.	OAIC investigation, fines and costly remediation	**Detected**
4	**Sensitive PII data stored in plaintext**	APP 11: Security	High breach risk if device is lost or compromised.	Breach remediation: $60k - $280k Legal costs + forensics: $150k+	**Detected**
5	**No visibility where sensitive data lives**	APP 1	The organisation is effectively blind as it cannot demonstrate where sensitive data lives, cyber insurers treat it as unmanaged risk.	Cyber insurers typically increase premiums 20- 70% at renewal and in a breach scenario the insurer may dispute or deny the payout.	**Detected**

Most Australian organisations underestimate the cost of a privacy breach.

The average cost of a breach is $4M

The reputational damage is severe: customer loss, media scrutiny, brand damage.. etc

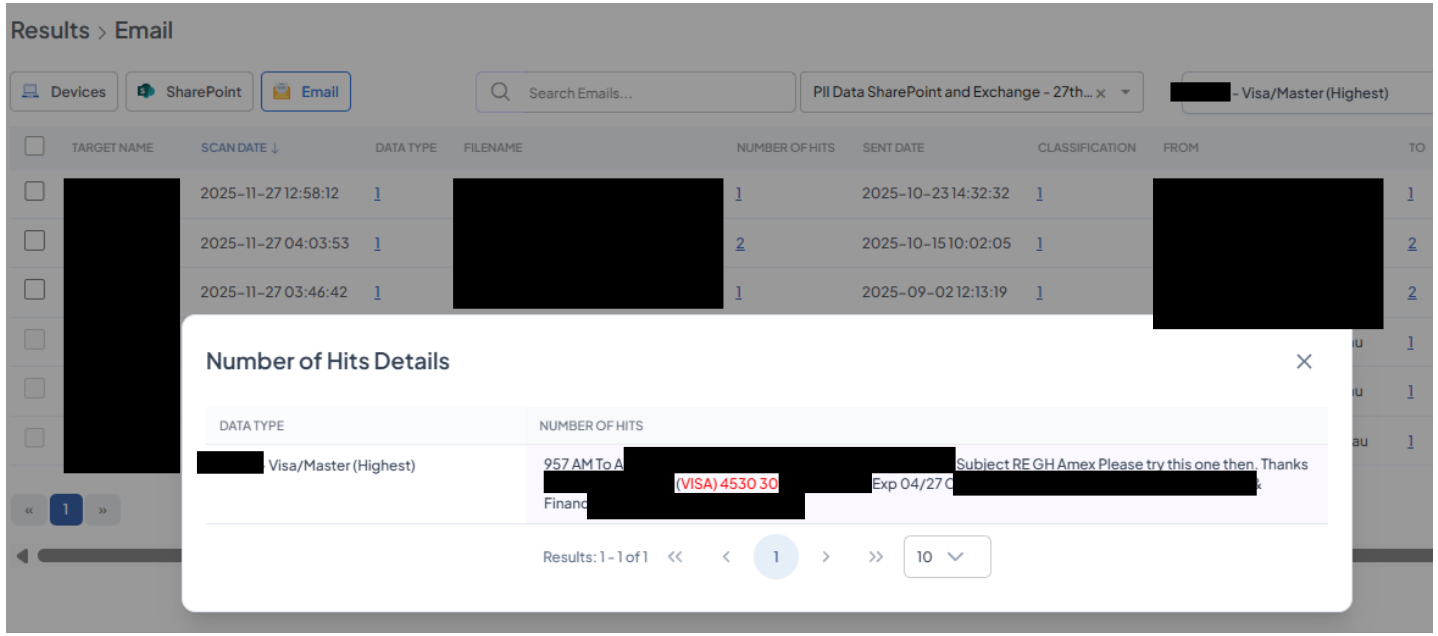
Storage of Credit Card Data Analysis

Credit Card Sensitive Information

1 What

Storage and Access of Sensitive Data		
Storage and Access of Credit Card details including CCV in an unsecure form.	**Technical control not implemented**	**High**

2 Evidence



3 Why it matters

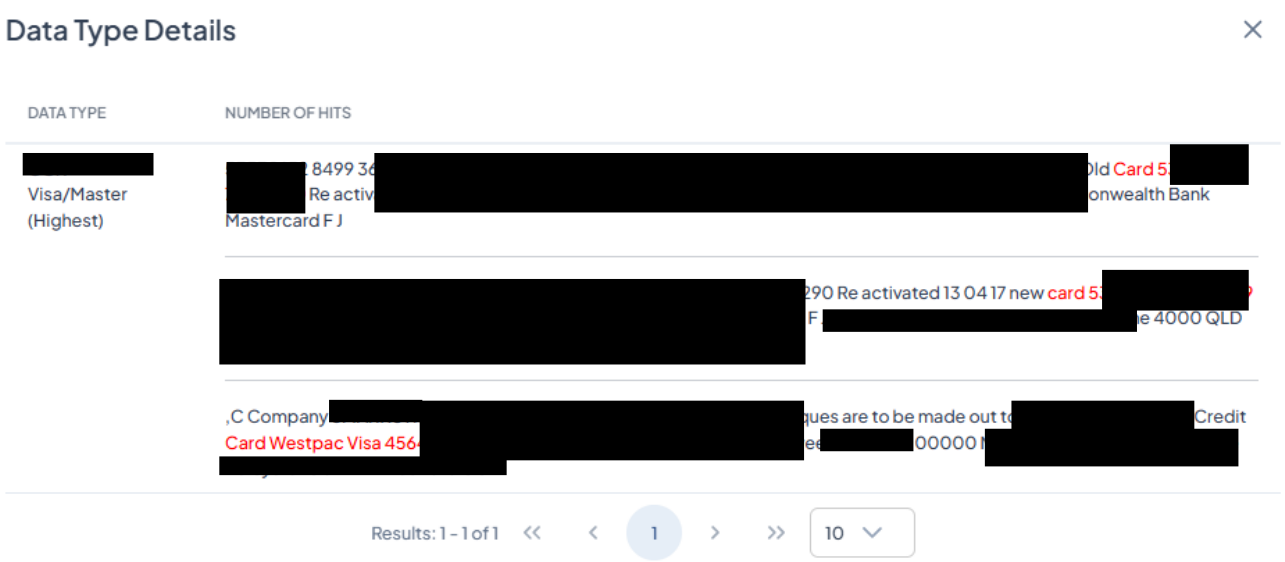
Anyone with access can misuse or steal the card data.

Risk: Creates a high financial fraud risk if the file is leaked, stolen or accidentally sent.

A lost or stolen laptop/computer becomes a data breach and potential violation under the Australian Privacy Act.

Credit Card Sensitive Information

2 Evidence



3 Why it matters

Anyone with access can misuse or steal the card data.

Risk: Creates a high financial fraud risk if the file is leaked, stolen or accidentally sent.

A lost or stolen laptop/computer becomes a data breach and potential violation under the Australian Privacy Act.

Stored Passwords and Credentials

Stored Passwords and Credentials

1 What

Stored Passwords and Credentials		
Risky data. Users detected storing credentials and plaintext password on images, documents and e-mails.	**Technical control not implemented**	**Very High**
Visibility of transfers. Visibility of sensitive staff data.	**Technical control not implemented**	**Very High**

2 Evidence

Data types

DATA TYPE	CONTEXT
[redacted] Username & Password (Medium)	by [redacted] Log in For existing customers username [redacted] com au Password c [redacted] member me Find my username Log in Reset my password TEXT EXTRACTION FAILED FileMetadata title Microsoft Outlook Memo Style author ,TEXT EXTRACTION FAILED Log in For existing customers username [redacted] k com au Password [redacted] Remember me Find my username Log in Reset my password TEXT EXTRACTION FAILED FileMetadata title Microsoft Outlook Memo Style author [redacted] u created date 2025 11 27T18 00 16 408084 modified

Results: 1 - 1 of 1 << < 1 > >> 10

3 Why it matters

Storing credentials in documents or images may be for legitimate reasons, but there are significant risks involved.

Risk: Can result in a breach and financial loss if data is exposed accidentally or due to malicious intent.

Stored Passwords and Credentials

2 Evidence

3 Why it matters

Storing credentials in documents or images may be for legitimate reasons, but there are significant risks involved.

Risk: Can result in a breach and financial loss if data is exposed accidentally or due to malicious intent.

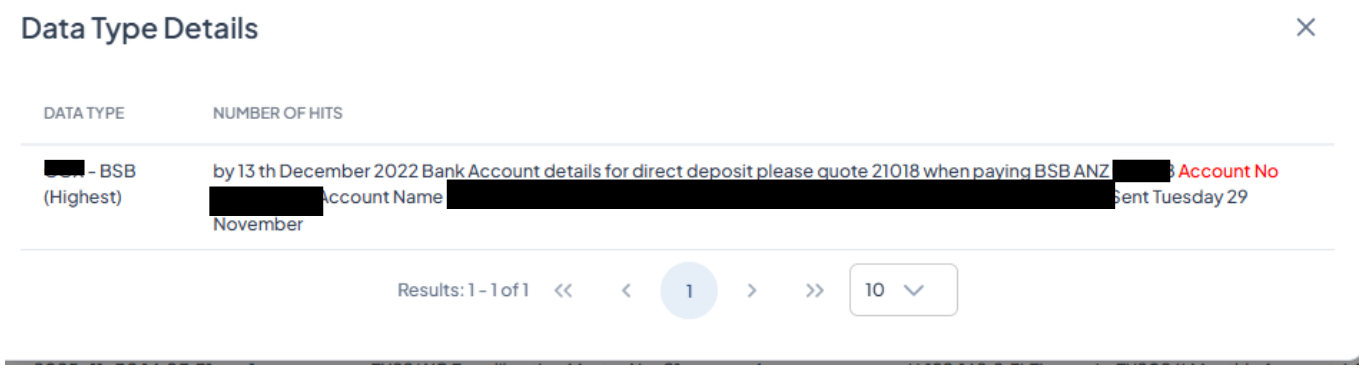
Australian Bank Account Number

Australian Bank Account Number

1 What

Storage and Access of Sensitive Data		
Storage and Access of sensitive data in plaintext.	Technical control not implemented	High

2 Evidence



3 Why it matters

Anyone with access can misuse or steal the data.

Risk: Creates a high financial fraud risk if the file is leaked, stolen or accidentally sent.

A lost or stolen laptop/computer becomes a data breach and potential violation under the Australian Privacy Act.

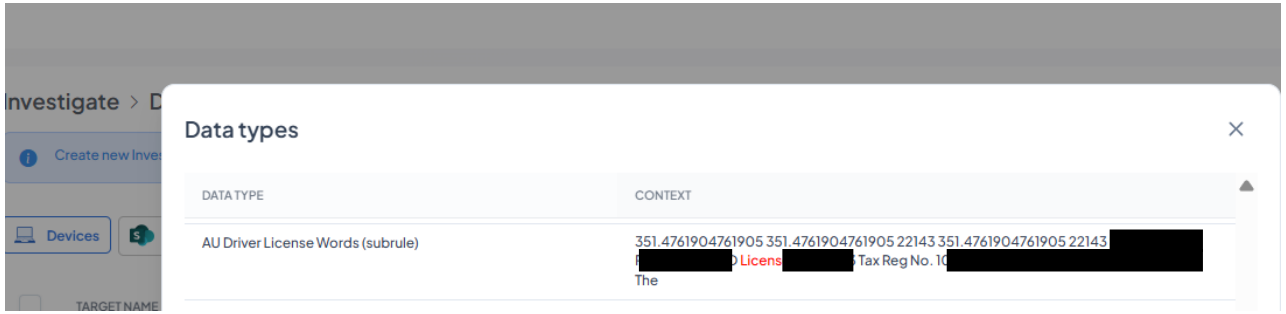
Australian Driver's License Number

Australian Drivers License Number

1 What

Storage and Access of Sensitive Data		
Storage and Access of sensitive data in plaintext.	Technical control not implemented	High

2 Evidence



3 Why it matters

Anyone with access can misuse or steal the data.

Risk: Creates a high financial fraud risk if the file is leaked, stolen or accidentally sent.

A lost or stolen laptop/computer becomes a data breach and potential violation under the Australian Privacy Act.

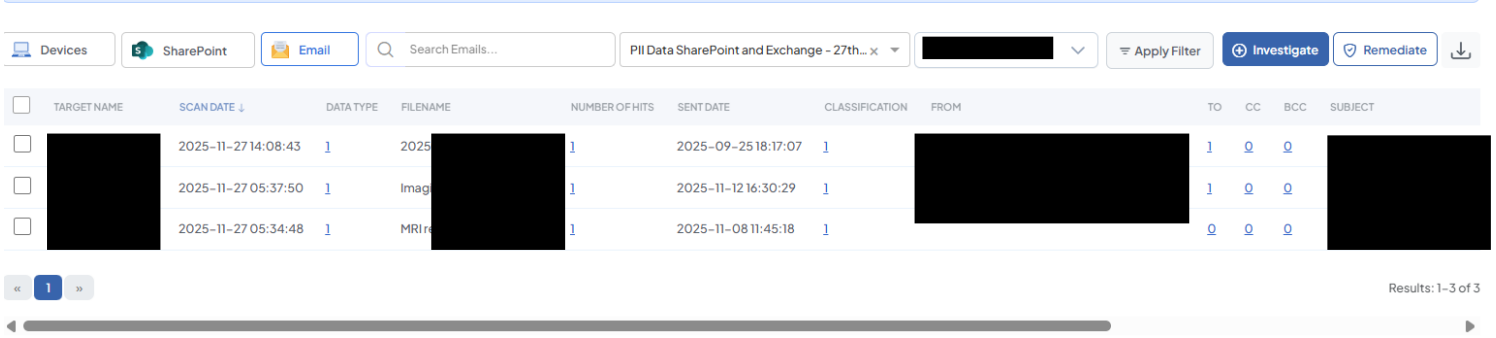
Australian Medicare Card Number

Australian Medicare Card Number

1 What

Storage and Access of Sensitive Data		
Storage and Access of sensitive data in plaintext.	Technical control not implemented	High

2 Evidence



3 Why it matters

Anyone with access can misuse or steal the data.

Risk: Creates a high financial fraud risk if the file is leaked, stolen or accidentally sent.

A lost or stolen laptop/computer becomes a data breach and potential violation under the Australian Privacy Act.

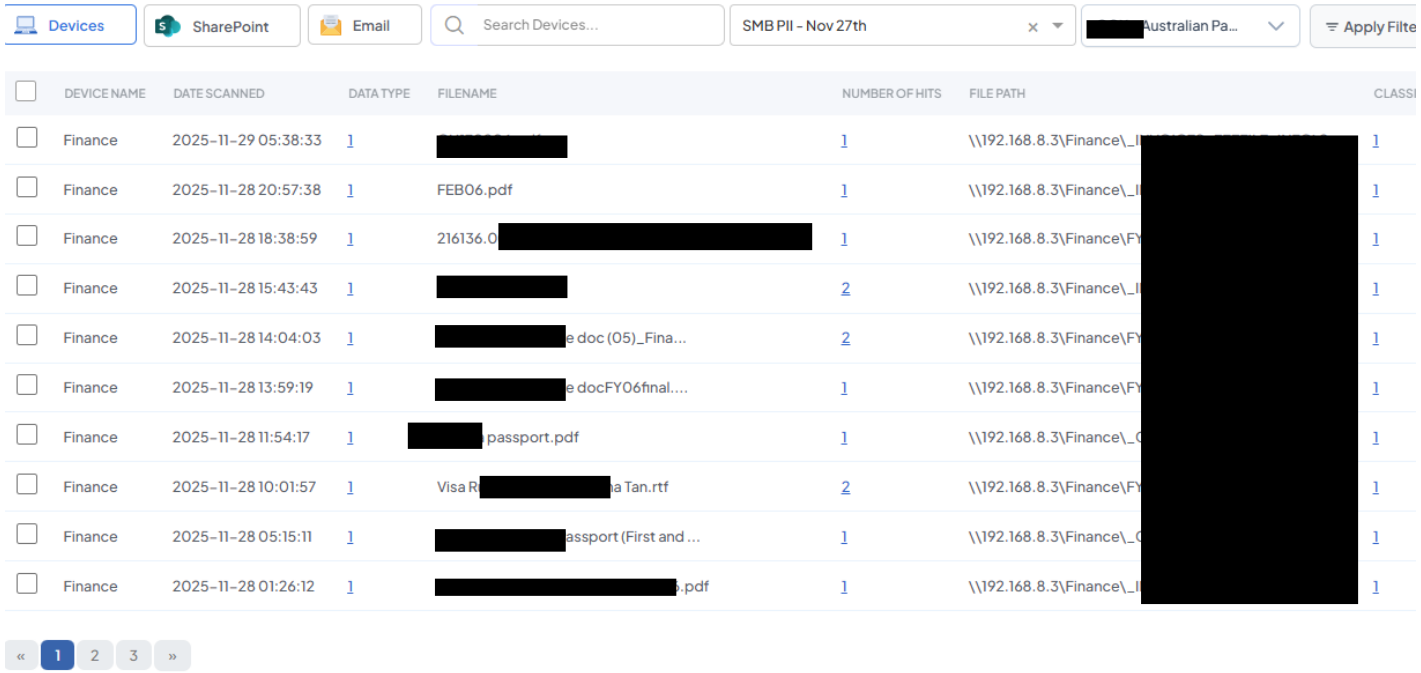
Australian Passport Number

Australian Passport Number

1 What

Storage and Access of Sensitive Data		
Storage and Access of sensitive data in plaintext.	**Technical control not implemented**	**High**

2 Evidence



3 Why it matters

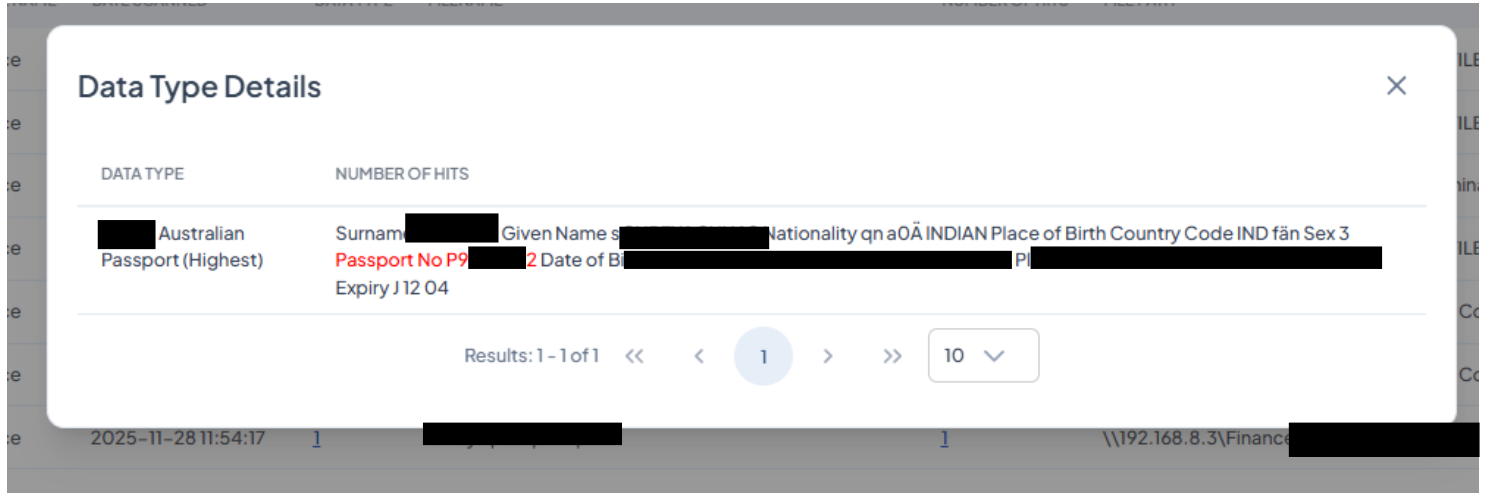
Anyone with access can misuse or steal the data.

Risk: Creates a high financial fraud risk if the file is leaked, stolen or accidentally sent.

A lost or stolen laptop/computer becomes a data breach and potential violation under the Australian Privacy Act.

Australian Passport Number

2 Evidence



3 Why it matters

Anyone with access can misuse or steal the data.

Risk: Creates a high financial fraud risk if the file is leaked, stolen or accidentally sent.

A lost or stolen laptop/computer becomes a data breach and potential violation under the Australian Privacy Act.

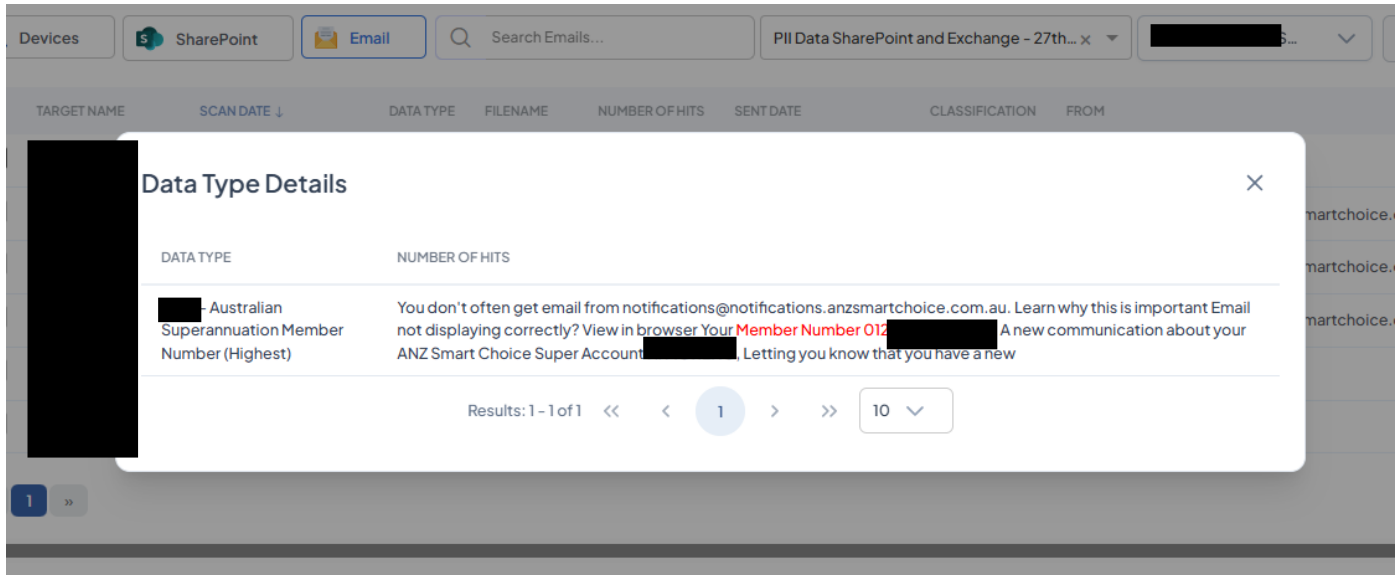
Australian Superannuation Identifier & Member

Australian Superannuation Identifier & Member

1 What

Storage and Access of Sensitive Data		
Storage and Access of sensitive data in plaintext.	**Technical control not implemented**	**High**

2 Evidence



3 Why it matters

Anyone with access can misuse or steal the data.

Risk: Creates a high financial fraud risk if the file is leaked, stolen or accidentally sent.

A lost or stolen laptop/computer becomes a data breach and potential violation under the Australian Privacy Act.

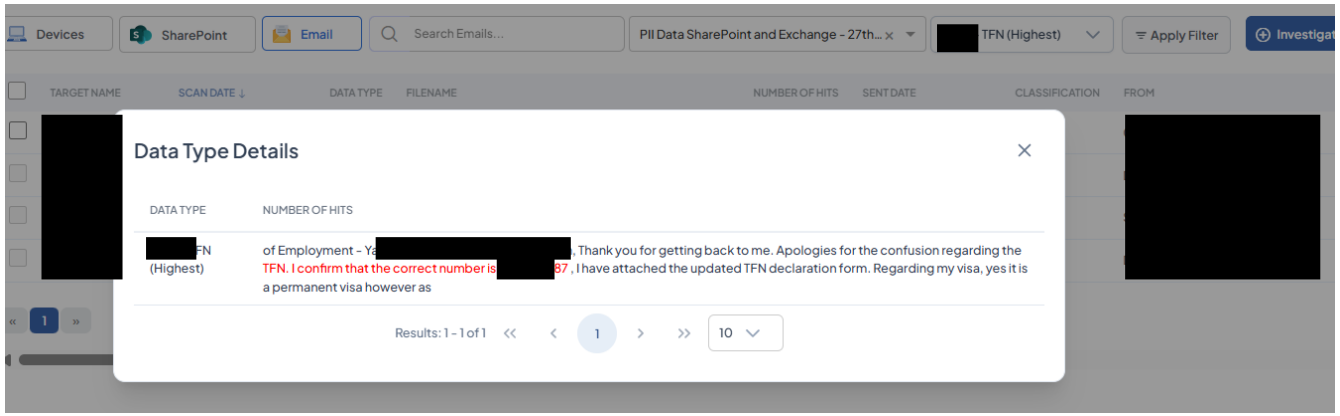
Australian Tax File Number (TFN)

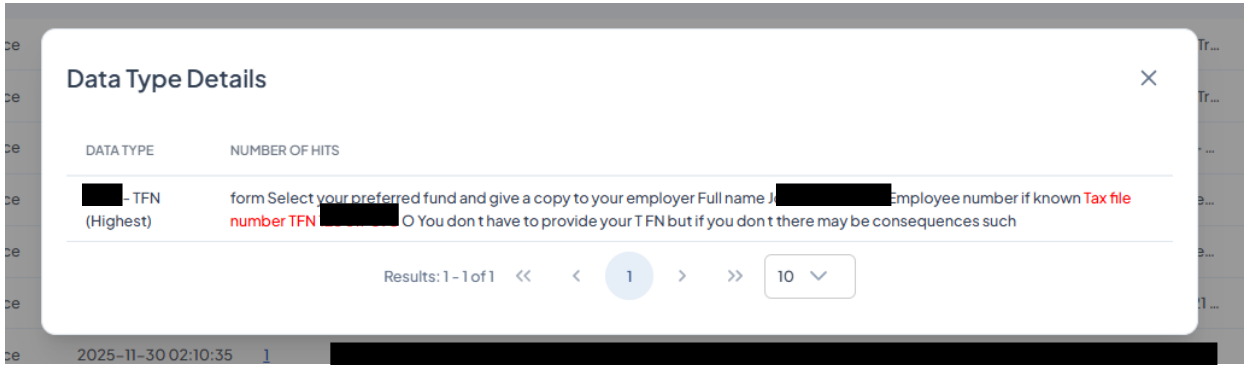
Australian Tax File Number (TFN)

1 What

Storage and Access of Sensitive Data		
Storage and Access of sensitive data in plaintext.	**Technical control not implemented**	**High**

2 Evidence





3 Why it matters

Anyone with access can misuse or steal the data.

Risk: Creates a high financial fraud risk if the file is leaked, stolen or accidentally sent.

A lost or stolen laptop/computer becomes a data breach and potential violation under the Australian Privacy Act.

Recommended Improvements

1 Immediate (0-30 days)

- Remediate risky data using GuardWare DISCOVER.
- Scan all shares, sites and mailboxes.
- Remove plaintext credentials.
- Move Credit Card processing to a PCI-compliant payment gateway instead of storing raw card data in spreadsheets.

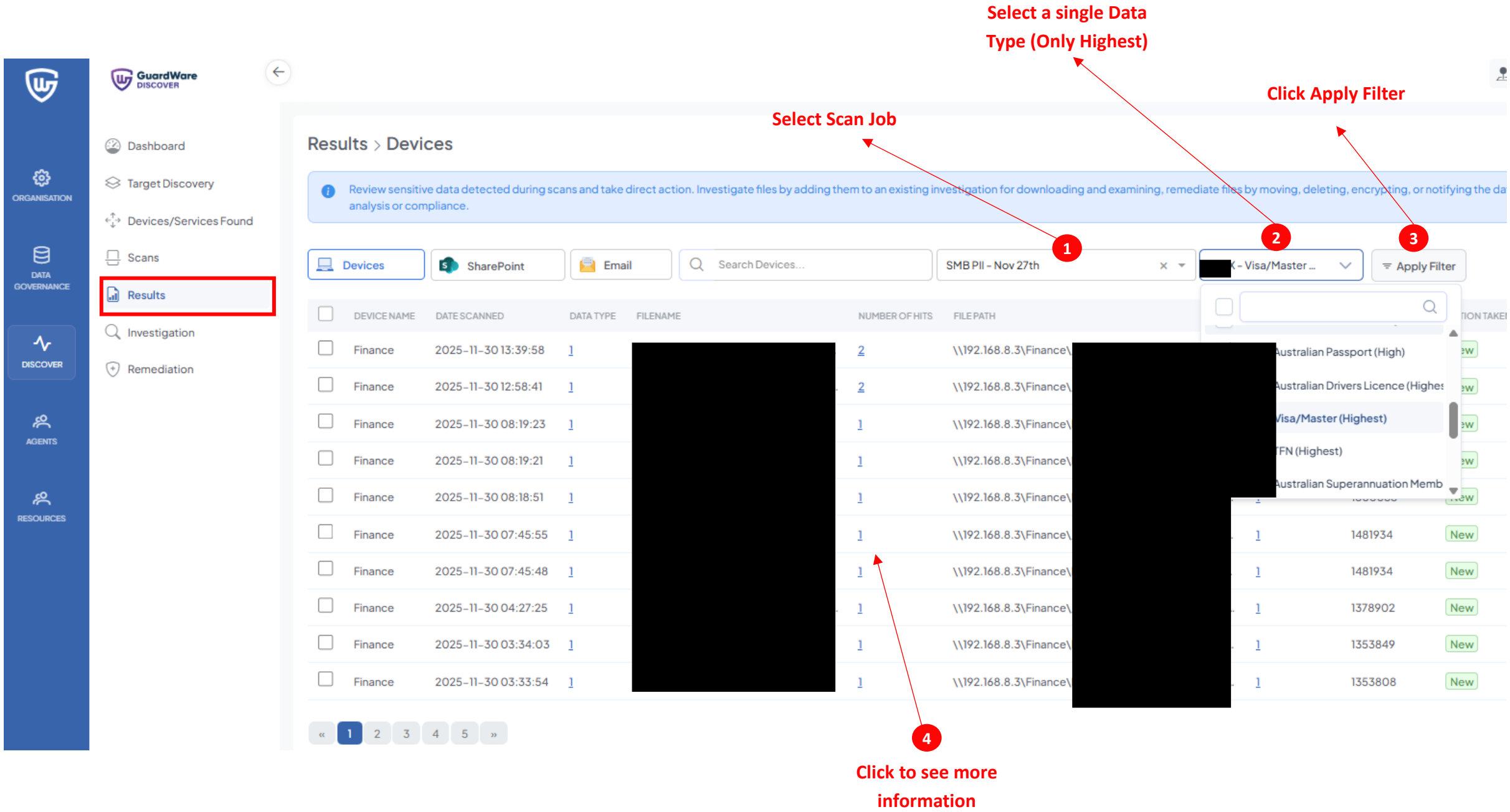
2 Medium-term (30-90 days)

- Conduct Data Privacy Training and Policy Awareness programs. GuardWare can help with automated policy awareness.
- Gain visibility into how data is accessed, moved and shared across the organization. Evidence capture to support Australian Data Privacy Act compliance. (GuardWare INSIGHT)
- Ensure sensitive data files remains persistently encrypted and destroyed if hacked or stolen. (GuardWare PROTECT)

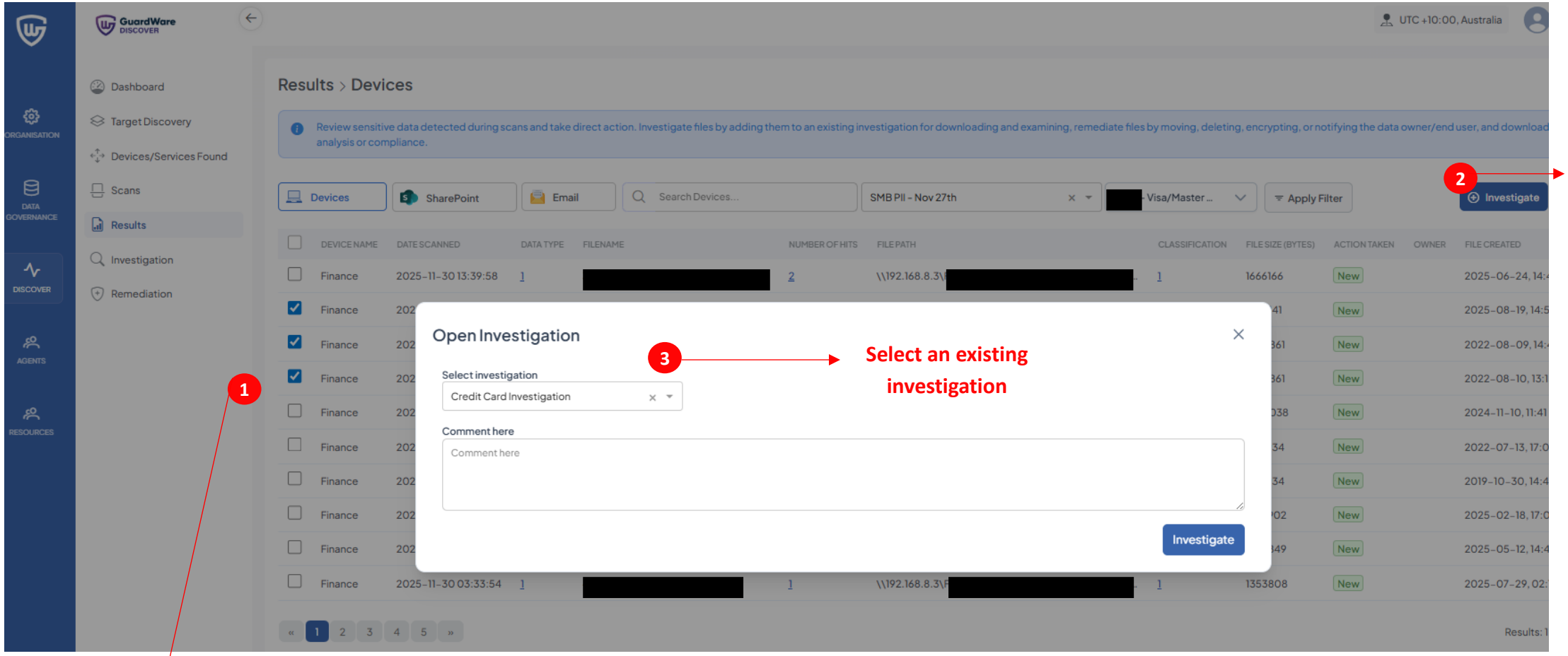
3 Long-term (90+ days)

- Develop an organisation-wide Data Governance Framework.
- Schedule quarterly PII & PCI scans.

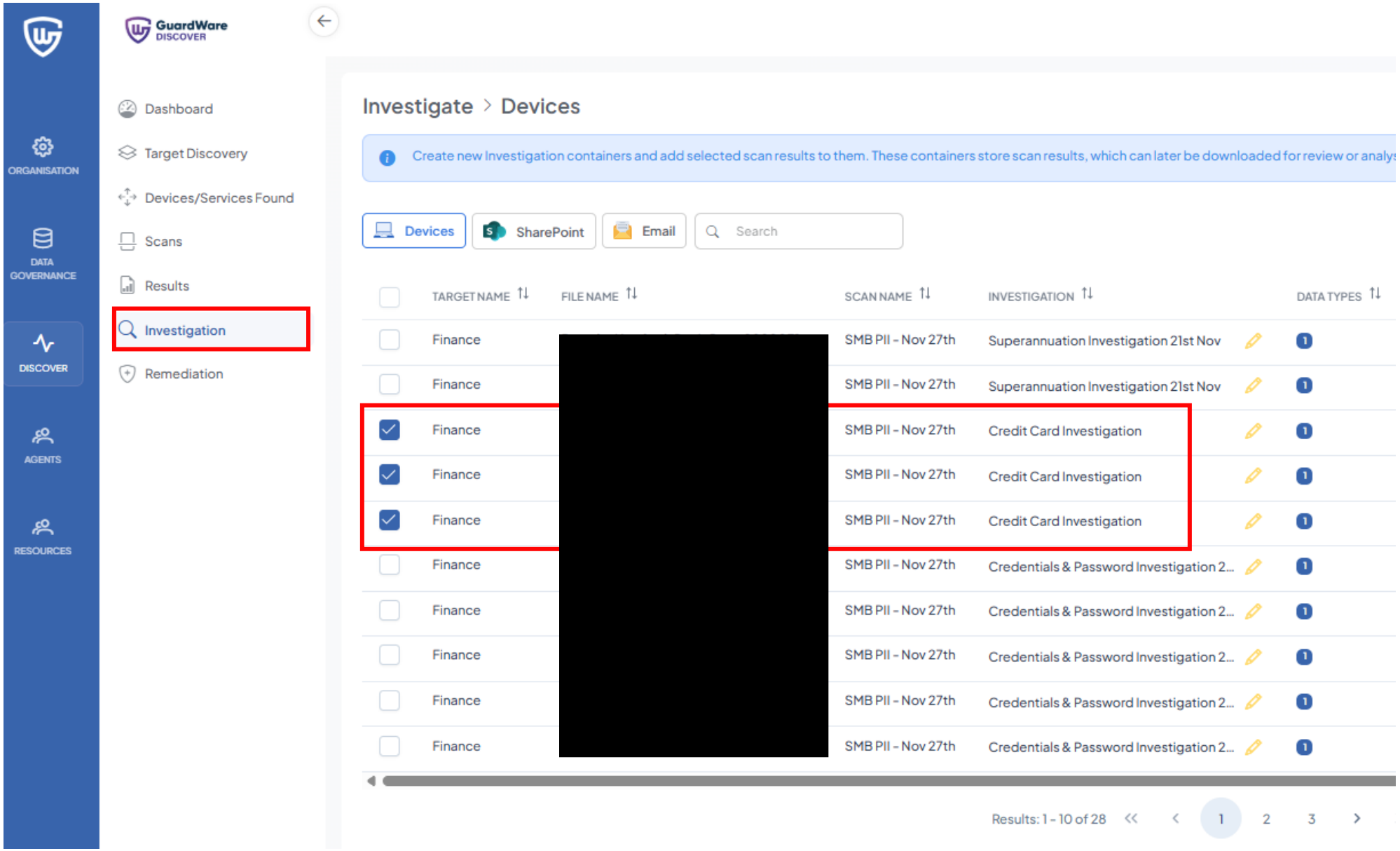
How to review initial results?



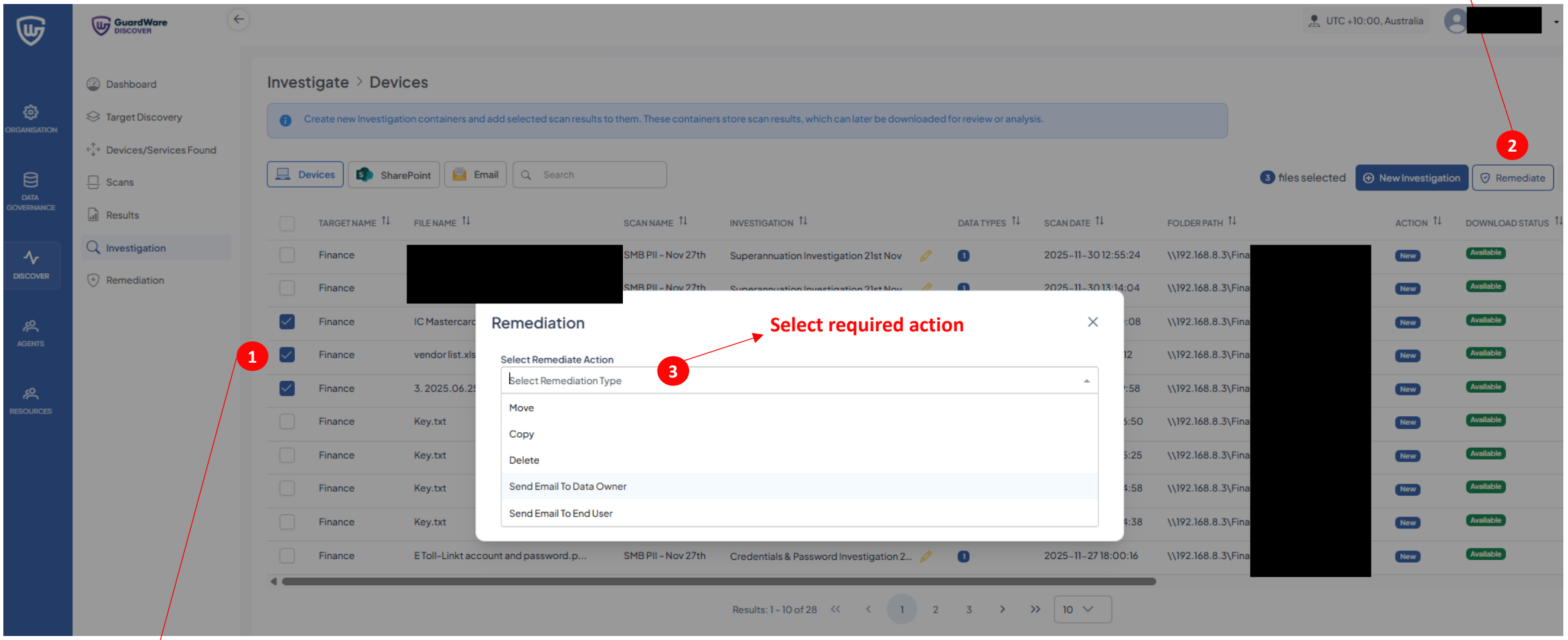
How to add files to an existing investigation?



How to check an open investigation?



How to remediate a file(s)?



GuardWare offers several products designed to keep your data safe and can help implement the recommendations in this report.