PRIVILEGED IDENTITY MANAGEMENT

Our Team

- Team

Dr. Sibi Chakkaravarthy Sethuraman

Tarun R

19BCN7122

Praveen K

19BCE7595

Nikhil V

19BCE7130

Why Not

- These lack integration
- Impractical for a broad user base

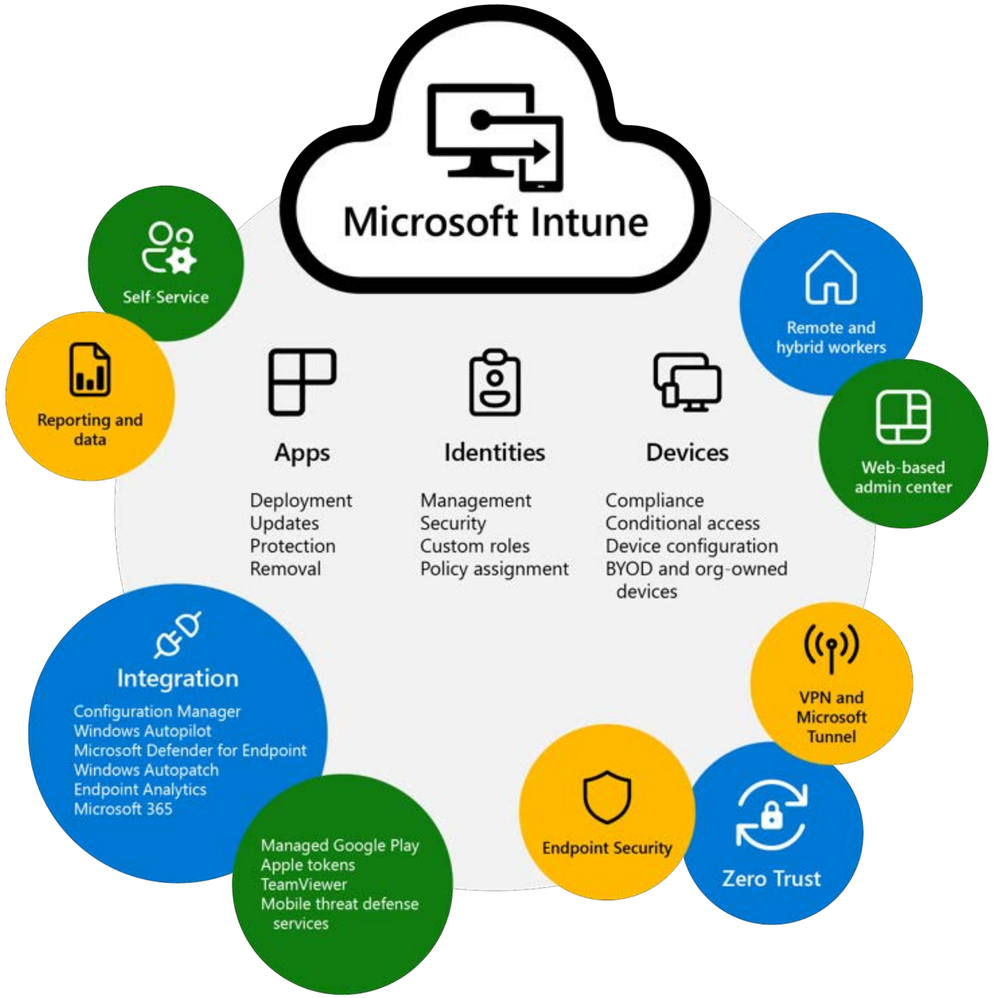
Antivirus

Deploying security orchestration tools

Encrypting Files

Firewall

Let's Combine



In our Journey

- Solution
- Results
- Benefits
- The Product

PCI DSS

Protect Cardholder Data

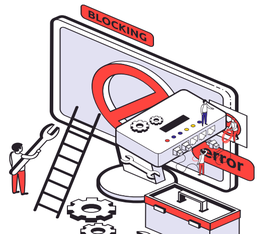
Build and Maintain a Secure Network and Systems

Maintain a Vulnerability Management Program

Regularly Monitor and Test Networks

Implement Strong Access Control Measures

Maintain an Information Security Policy



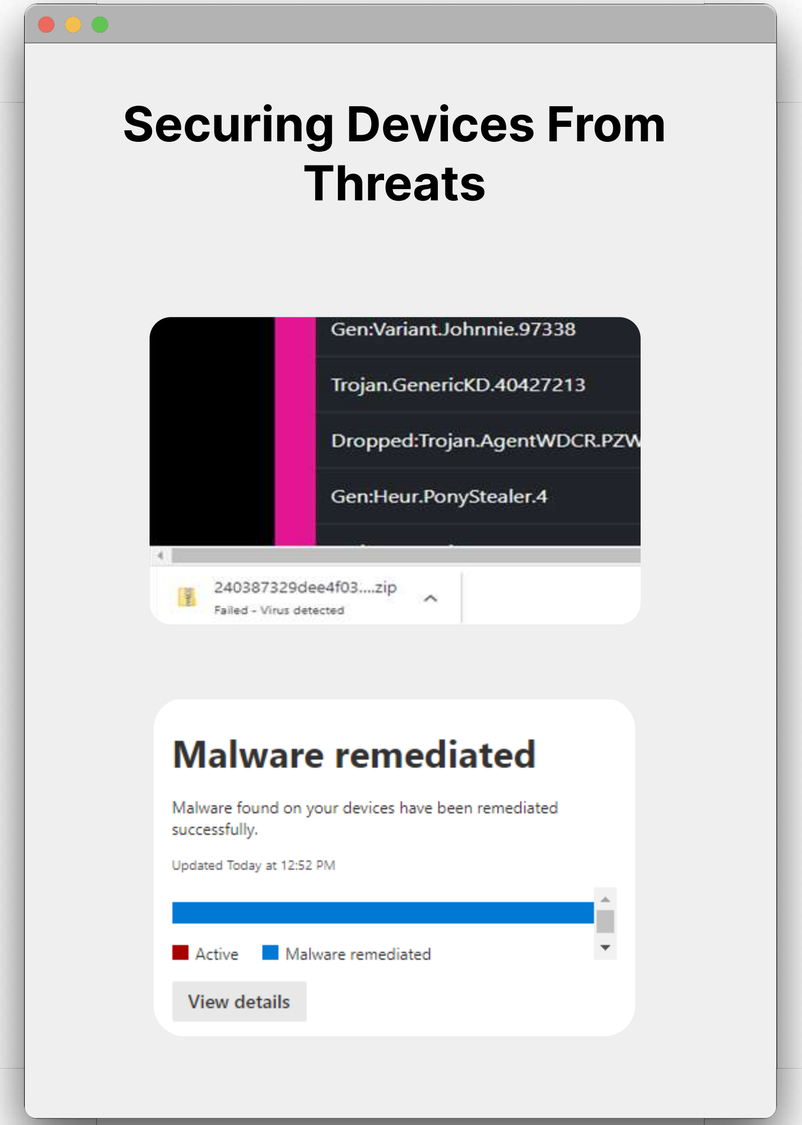
Too Many

- Monitor account activity
- Apply sensitivity labels to protect personal data
- Use limited administrative rol
- Update antivirus definitions
- Recall emails to unintended recipients or with unintended attachments
- Implem
- Resume full disk encryption on all drives
- Disable Print Spooler Service on domain controllers

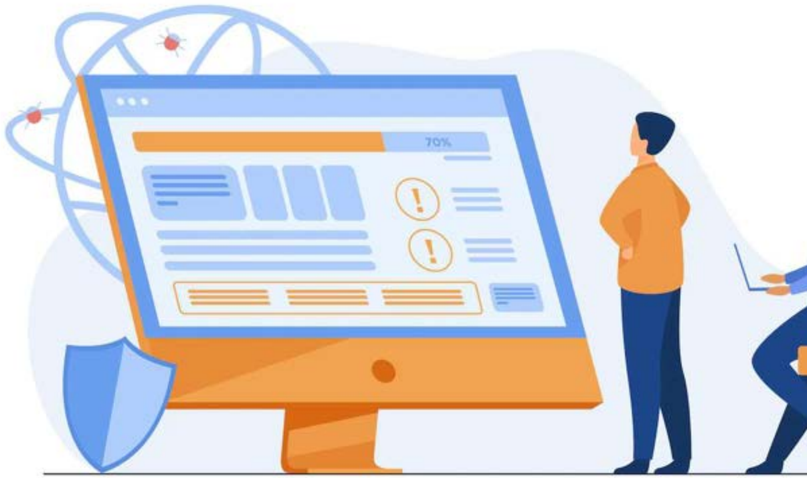
What are these for?

- Monitor account activity
- Protect against spoofing and phishing emails
- Review automated alerts
- Implement passwordless authentication for shared machines or highly privileged identities
- Conceal information with lock screen
- Create customized DLP policies for sensitive financial data
- Monitor

The Devices

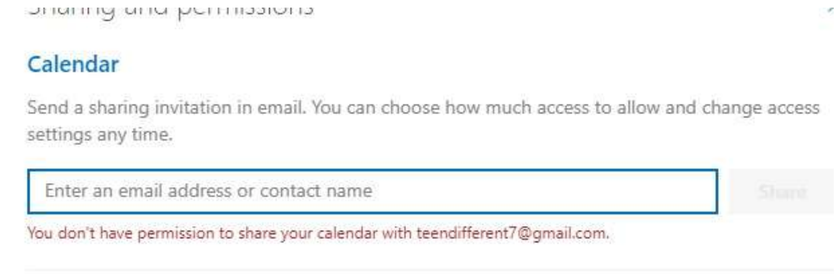


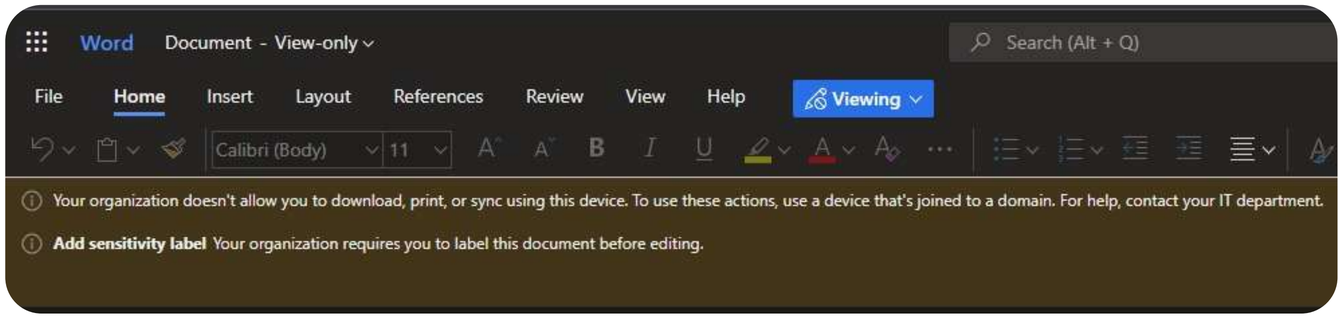
- Protection against malware, spyware.
- Detects and blocks threats (online & offline)
- Alerts the security team



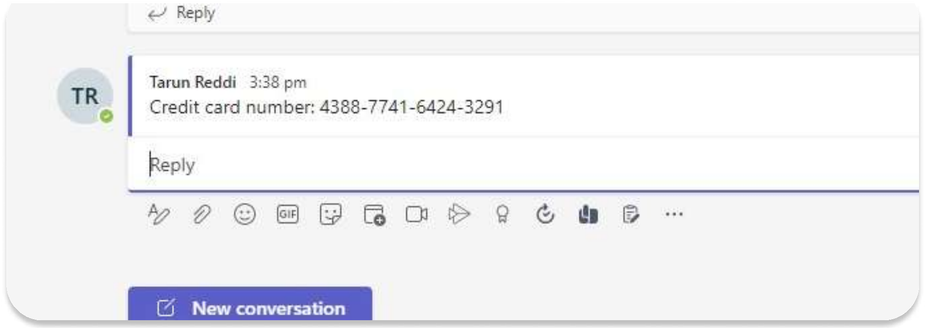
Applications

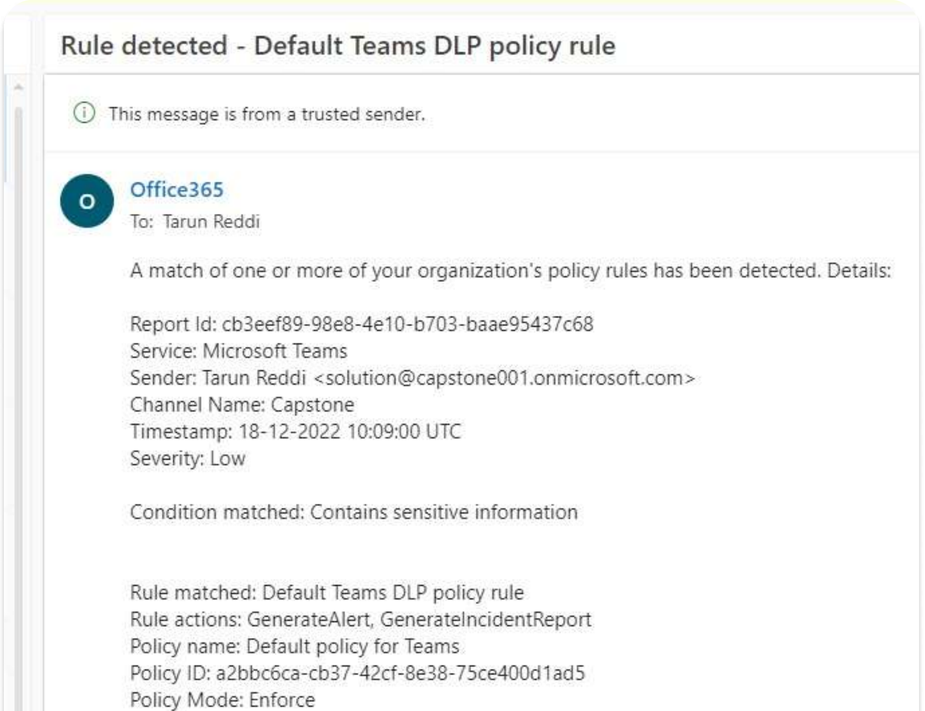
- Selected applications can process the data.
- Applications restricted to print, sync or download.
- Limited to view only, when its accessed through external devices.
- Data can only be shared within the organization's addresses.



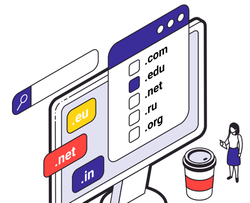


Alerts



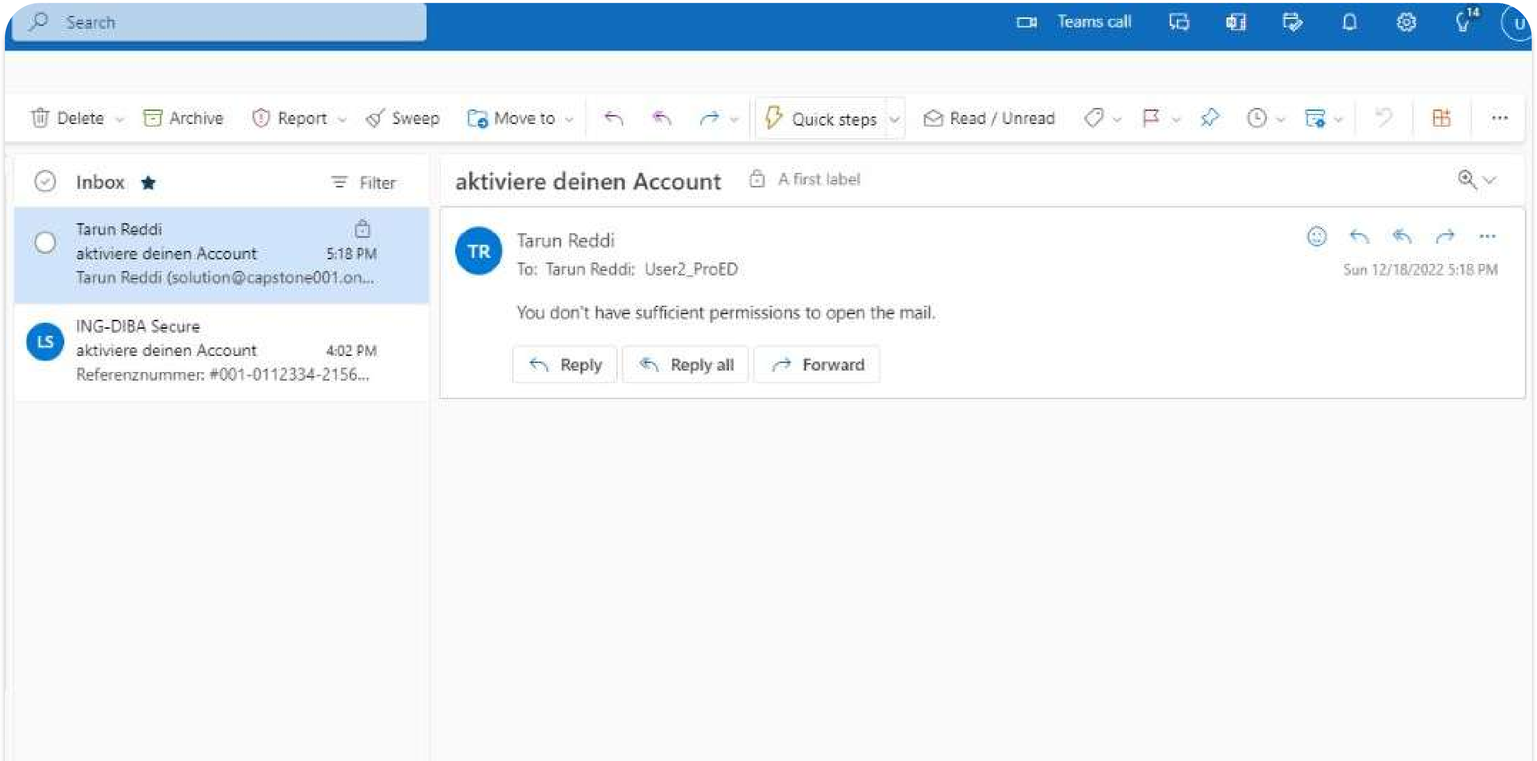


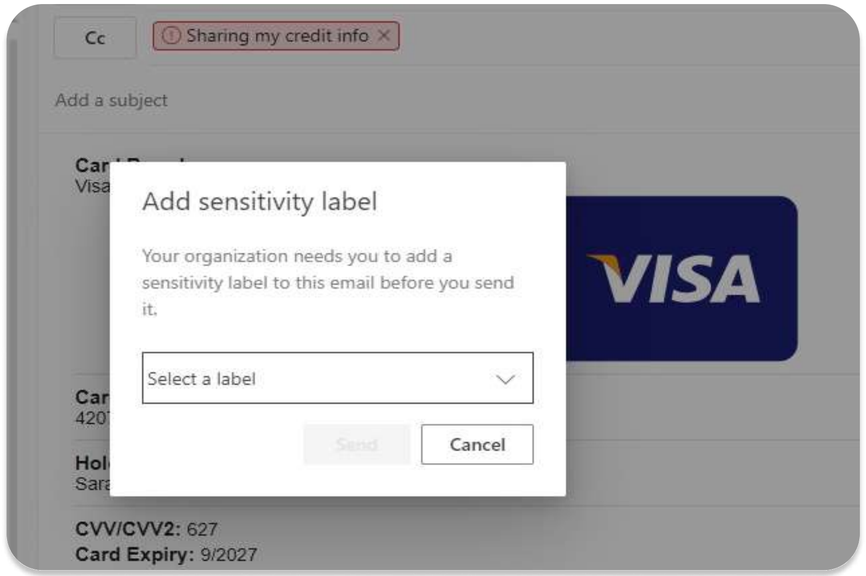
- Automated alerts, when sensitive information detected.
- Prevents data leak through emails, group discussions, teams, etc.



Mitigates

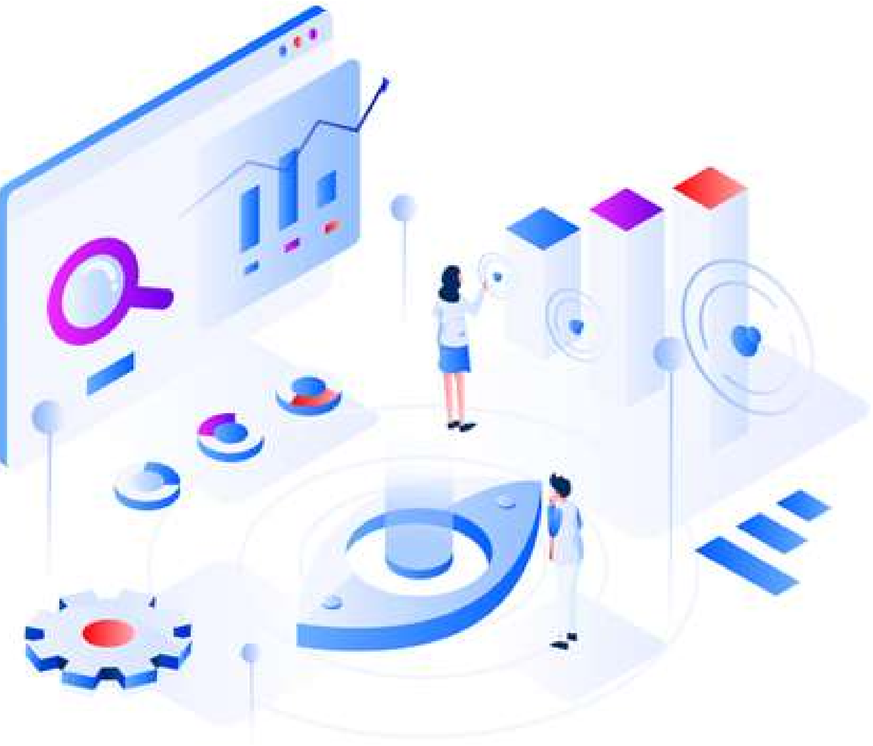
- Detects Spam, phishing emails
- Restrict employees from viewing phishing emails
- Alerts the security dep/ admin
- Helpful in monitoring the frequency of these emails

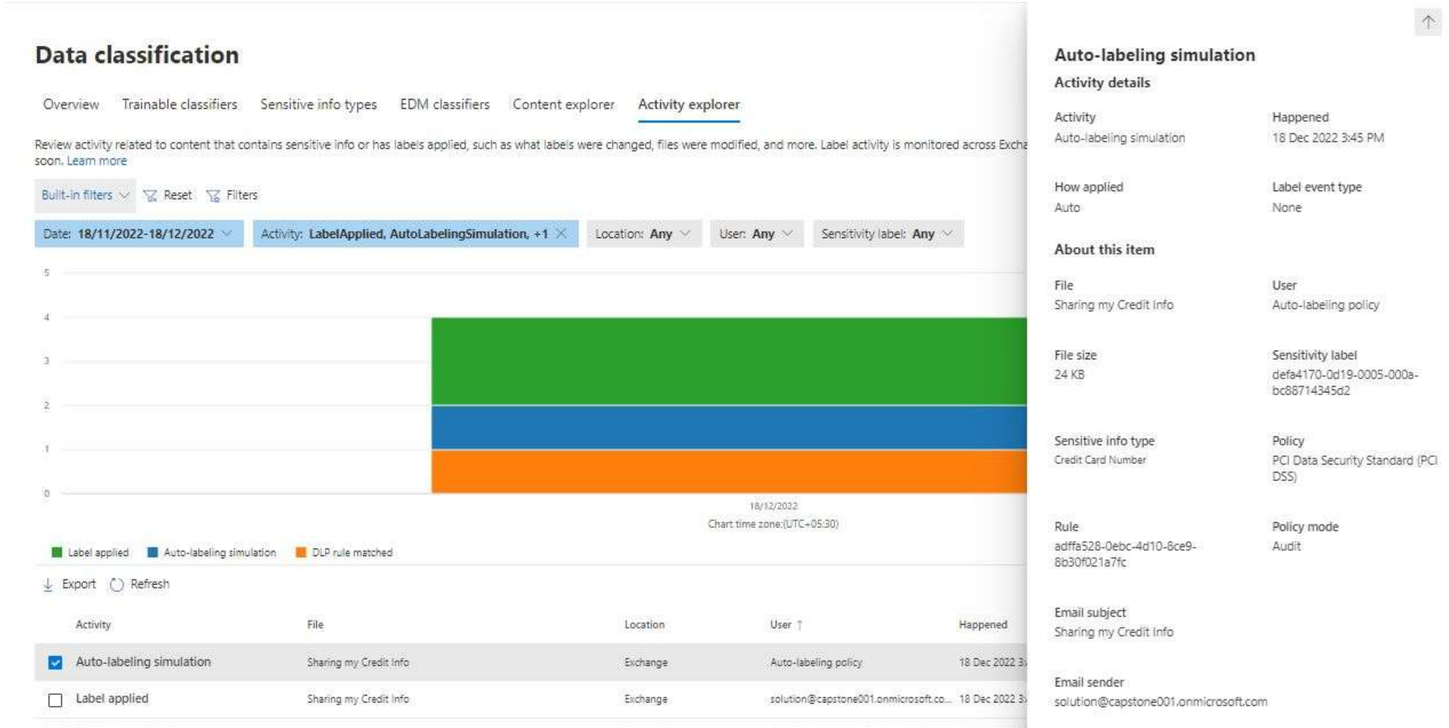




Tracks

- Prevents sharing without labelling the data.
- Gives the the admin what data is being shared to whom
- Automatic labelling You don't need to train your users when to use each of your classifications.
- You don't need to rely on users to classify all content correctly.
- Users no longer need to know about your policies—they can instead focus on their work.





All in one

A Zero Trust Solution

- Protect your data
- Know your data
- Prevent data loss
- Manage your data lifecycle
- Identify data risks and manage regulatory compliance requirements
- Detect and act on risk activities with insider risk management
- Restrict communication and collaboration between users with information barriers

Our Product

For 100$ only

- Understand PIM
- Understand about subscriptions
- Design your solution
- Configuration
- Testing the Configurations