

PRIVILEGED IDENTITY MANAGEMENT





Our Team

- Team



**Dr. Sibi Chakkaravarthy
Sethuraman**



Tarun R
19BCN7122



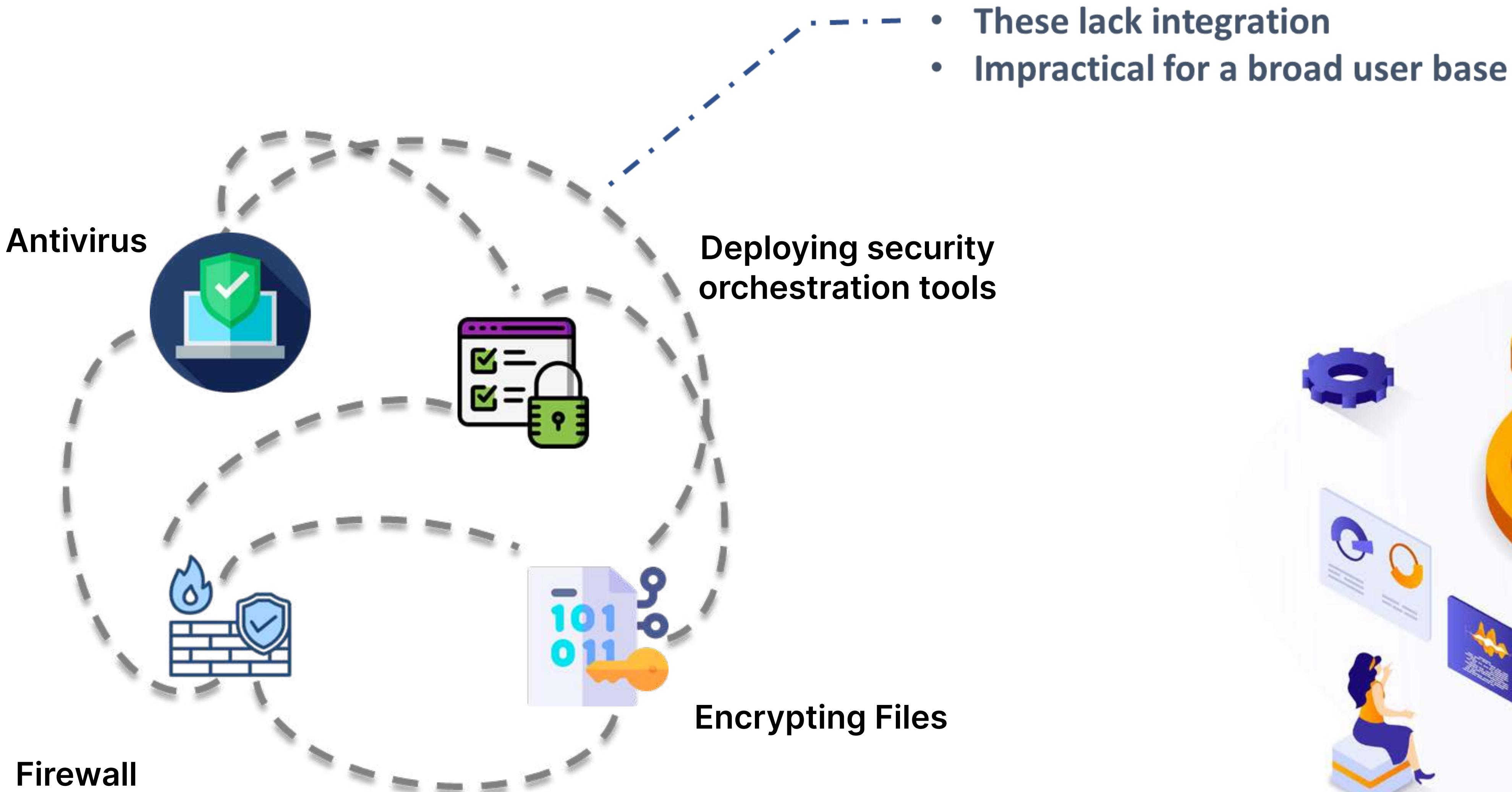
Praveen K
19BCE7595



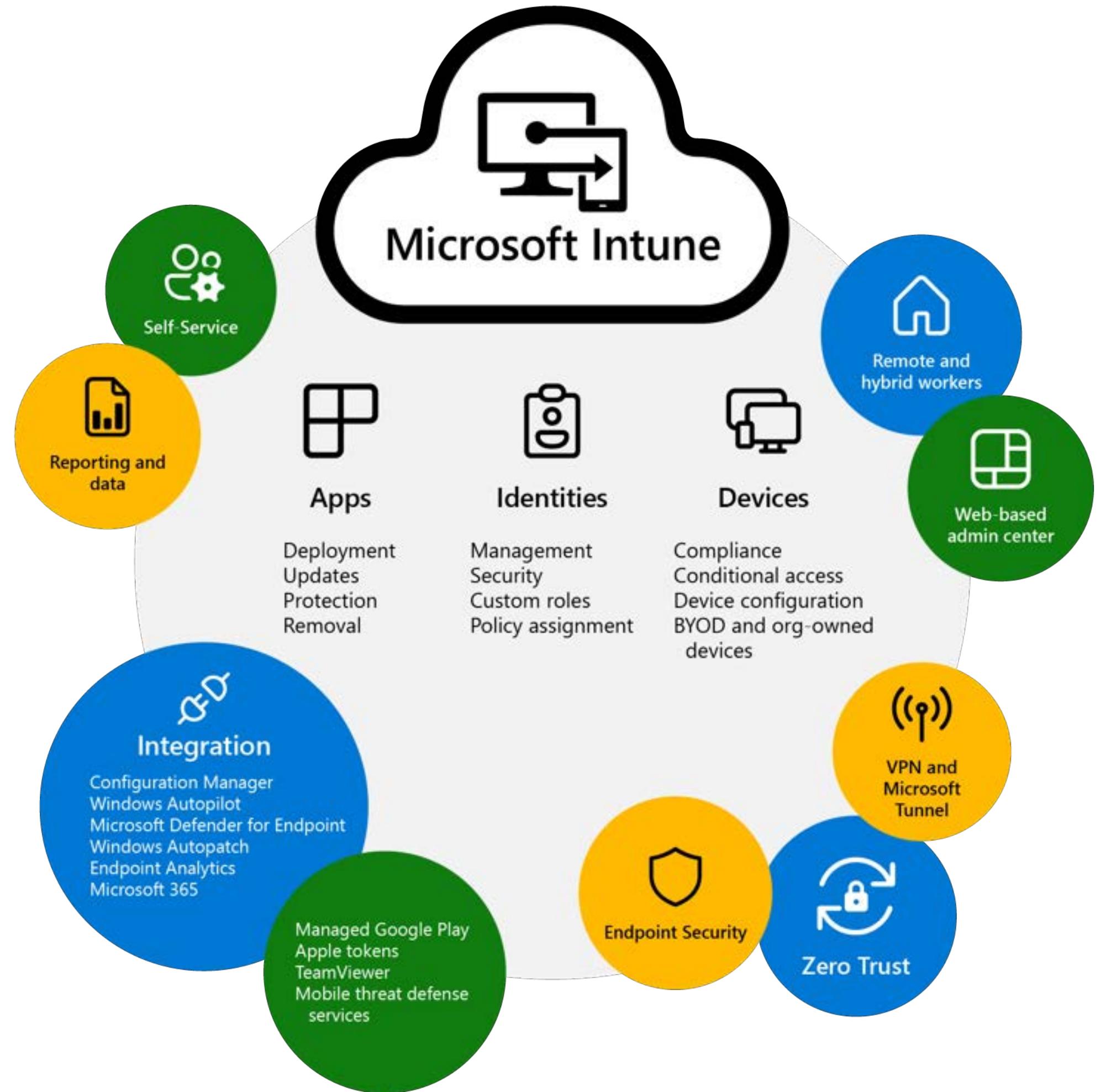
Nikhil V
19BCE7130



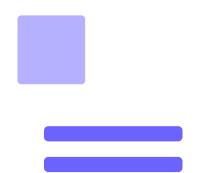
Why Not



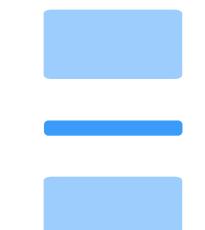
Let's Combine



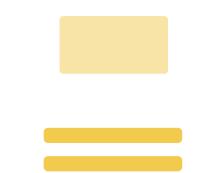
In our Journey



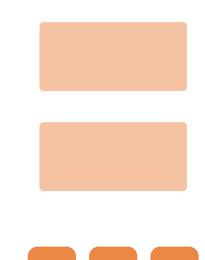
Solution



Results



Benefits

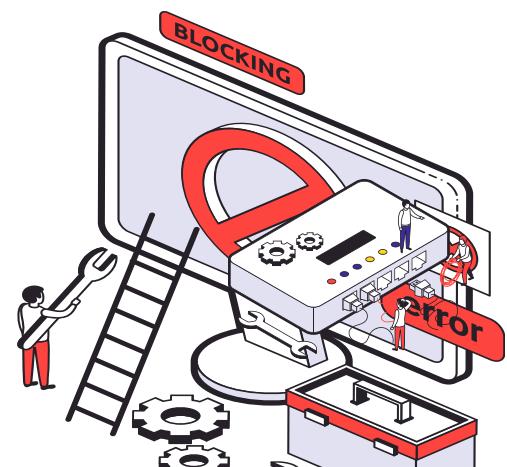
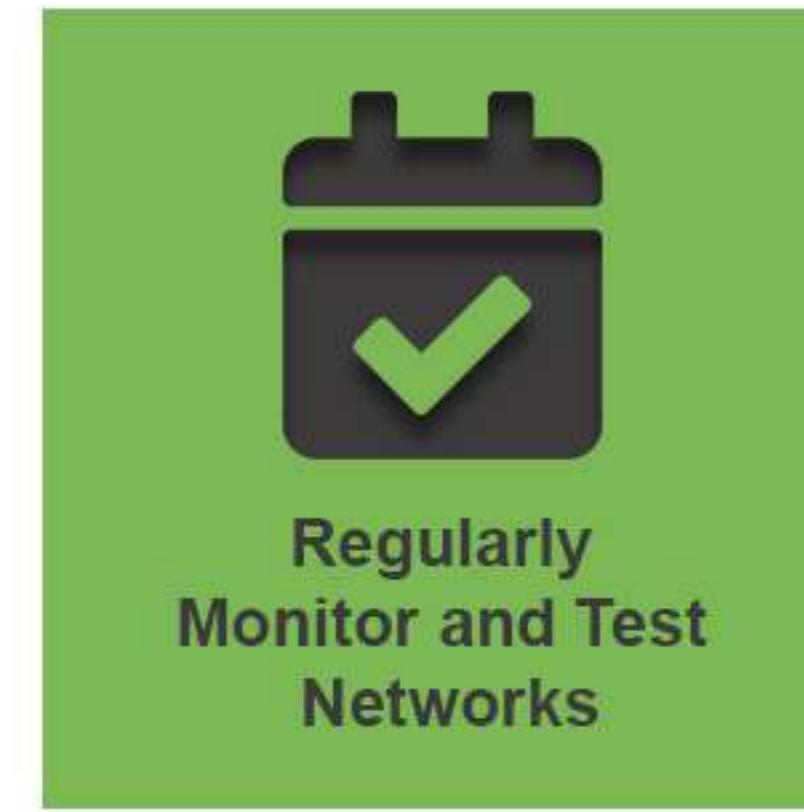
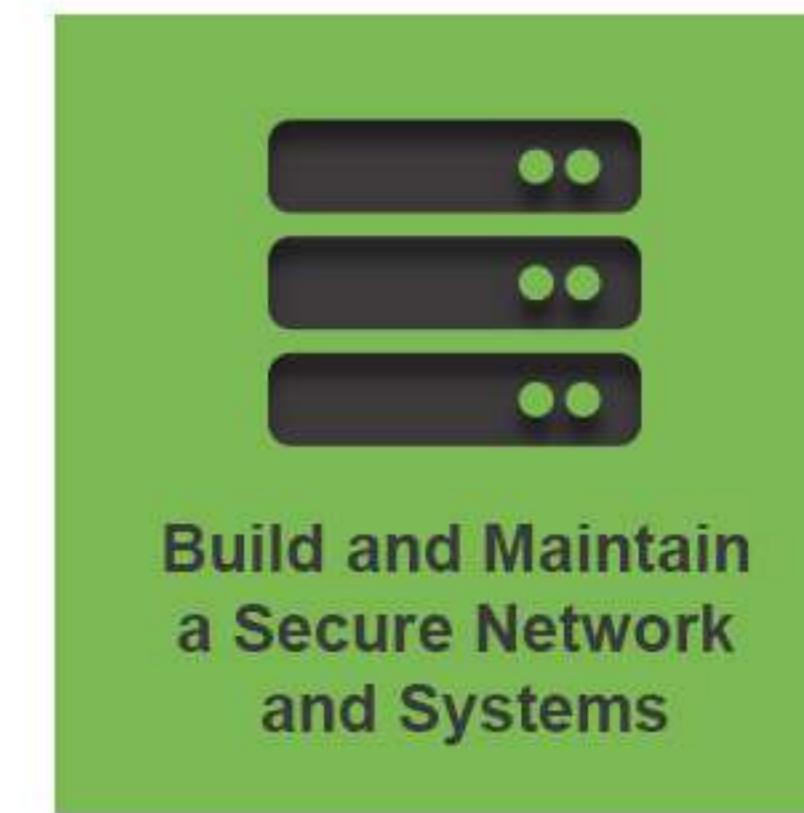
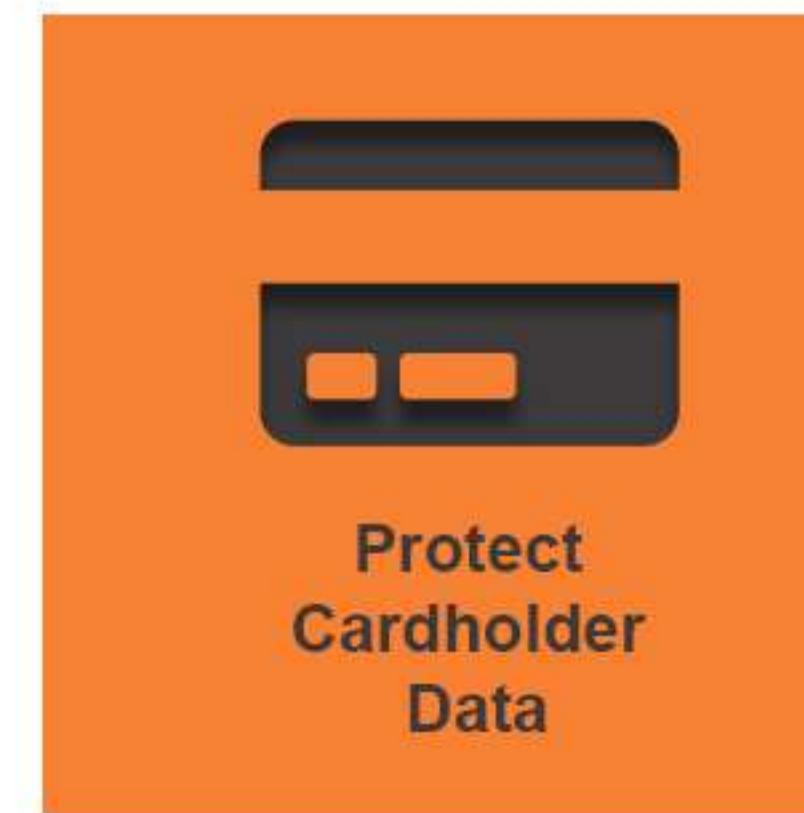


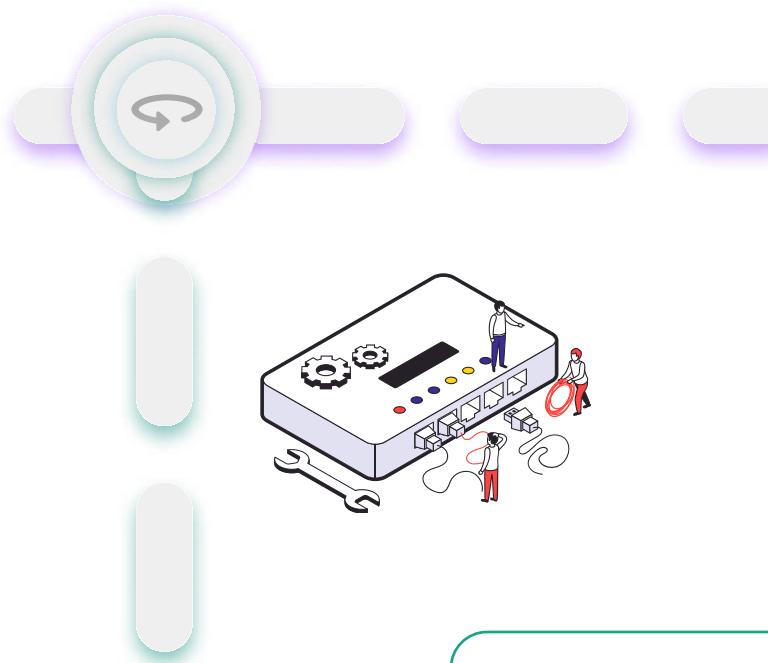
The Product



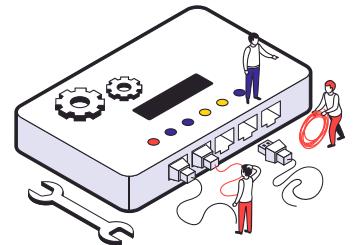


PCI DSS





Too Many



Monitor account activity



Apply sensitivity labels to protect personal data



Use limited administrative roles



Update antivirus definitions



Recall emails to unintended recipients or with unintended attachments



Implement



Resume full disk encryption on all drives



Disable Print Spooler Service on domain controllers



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

The screenshot shows a window titled "Securing Devices From Threats". At the top, there's a list of detected threats:

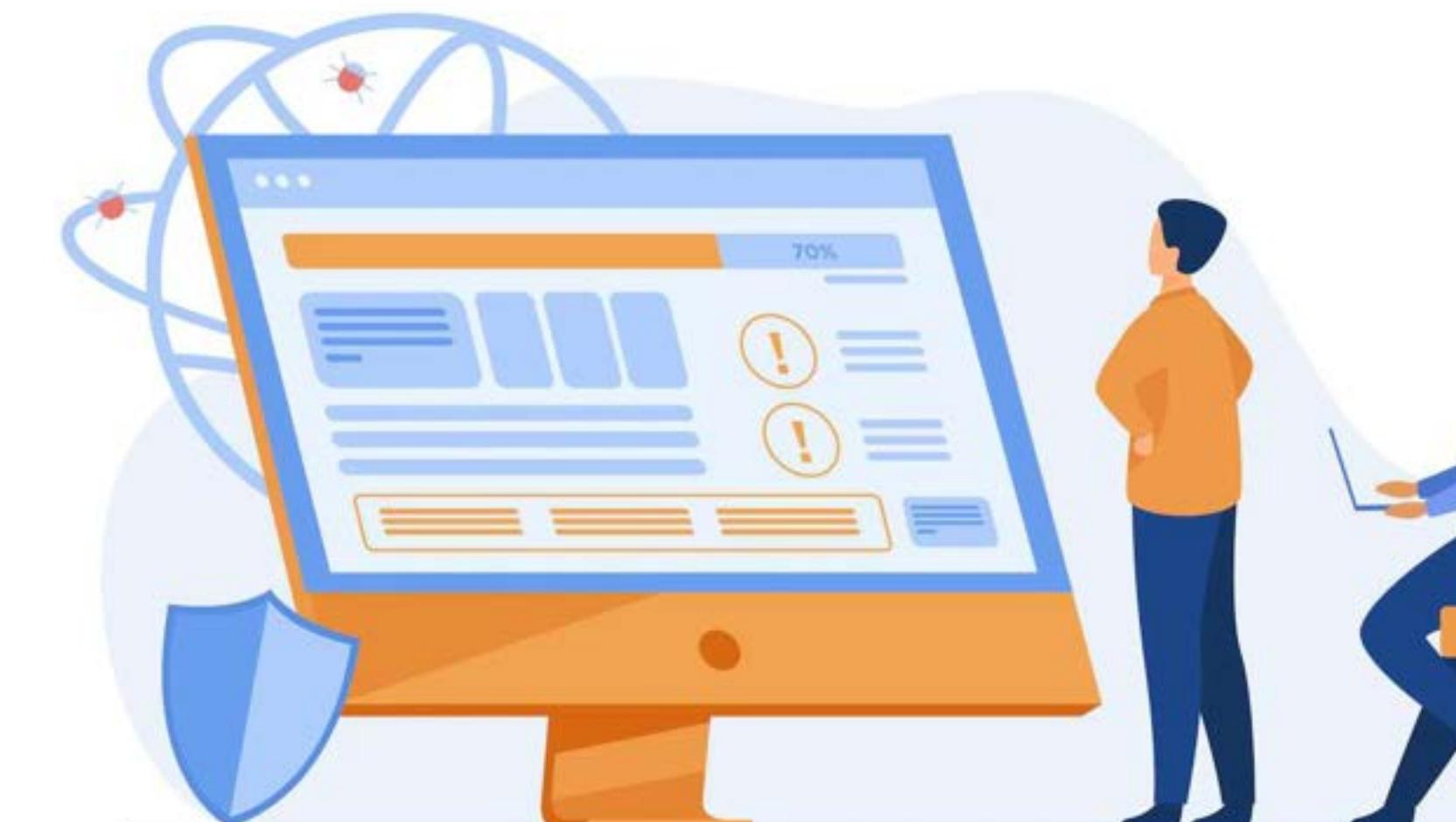
- Gen:Variant.Johnnie.97338
- Trojan.GenericKD.40427213
- Dropped:Trojan.AgentWDCR.PZW
- Gen:Heur.PonyStealer.4

Below this is a file download interface showing a failed attempt:

240387329dee4f03....zip
Failed - Virus detected

At the bottom, a summary box states "Malware remediated" with the message: "Malware found on your devices have been remediated successfully." It includes a timestamp "Updated Today at 12:52 PM" and a progress bar indicating 70% completion, with "Active" in red and "Malware remediated" in blue. A "View details" button is also present.

- 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.

Sharing and permissions

Calendar

Send a sharing invitation in email. You can choose how much access to allow and change access settings any time.

Enter an email address or contact name Share

You don't have permission to share your calendar with teendifferent7@gmail.com.

Word Document - View-only

File Home Insert Layout References Review View Help Viewing

Calibri (Body) 11 A A B I U A A A ...

Your organization doesn't allow you to download, print, or sync using this device. To use these actions, use a device that's joined to a domain. For help, contact your IT department.

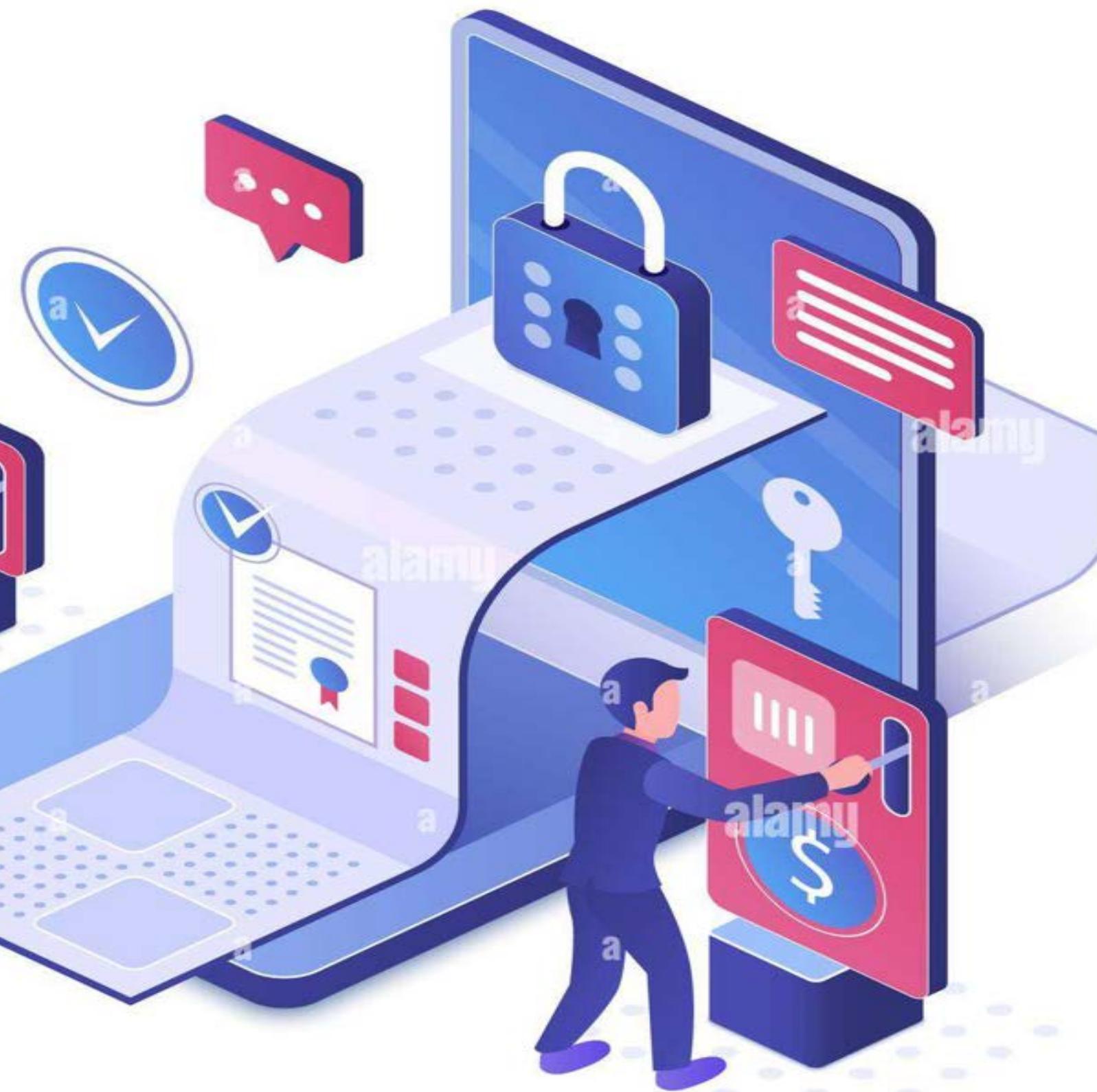
Add sensitivity label Your organization requires you to label this document before editing.



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



Inbox

Tarun Reddi aktiviere deinen Account 5:18 PM

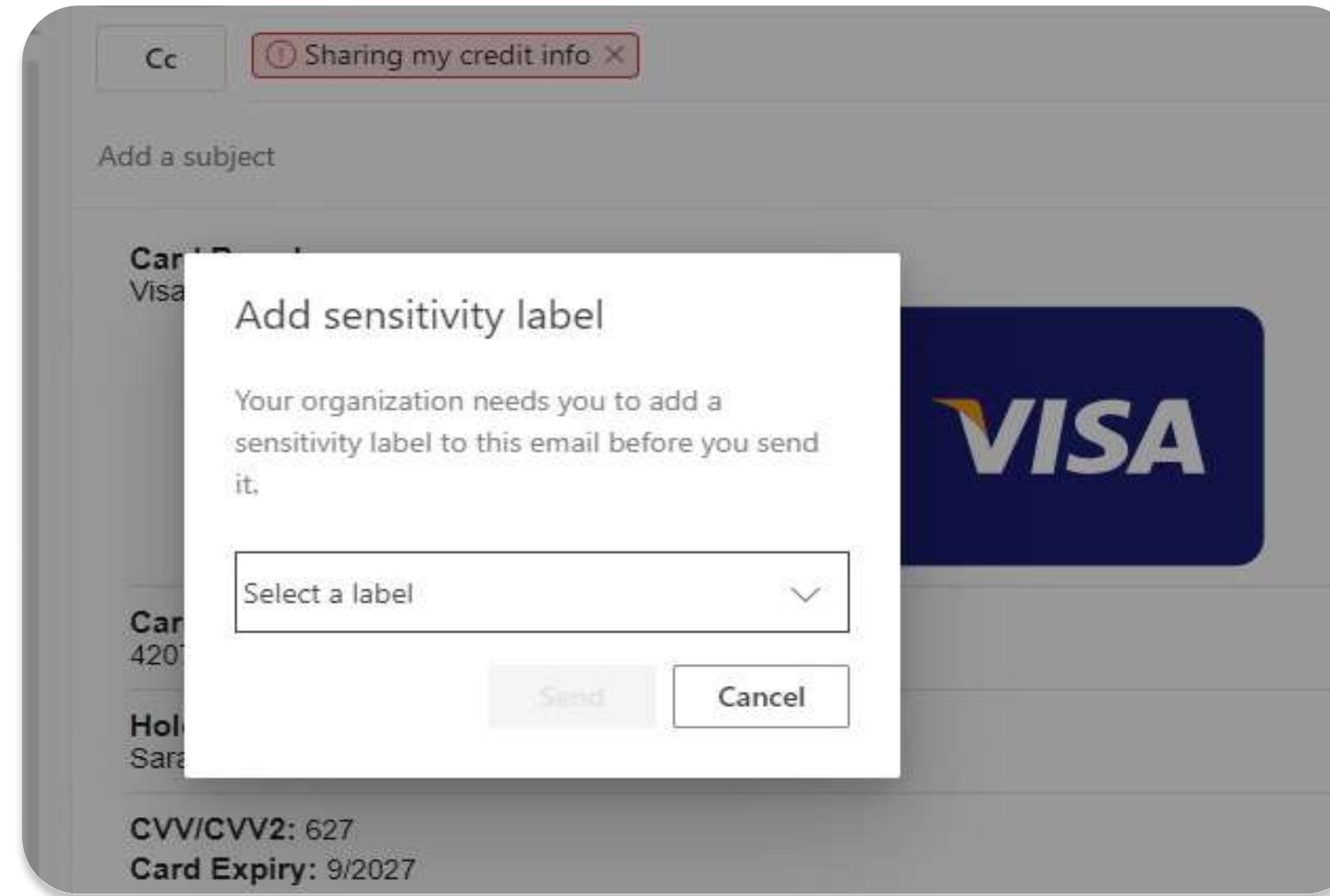
ING-DIBA Secure aktiviere deinen Account 4:02 PM

TR Tarun Reddi To: Tarun Reddi: User2_ProED Sun 12/18/2022 5:18 PM

You don't have sufficient permissions to open the mail.

Reply Reply all Forward

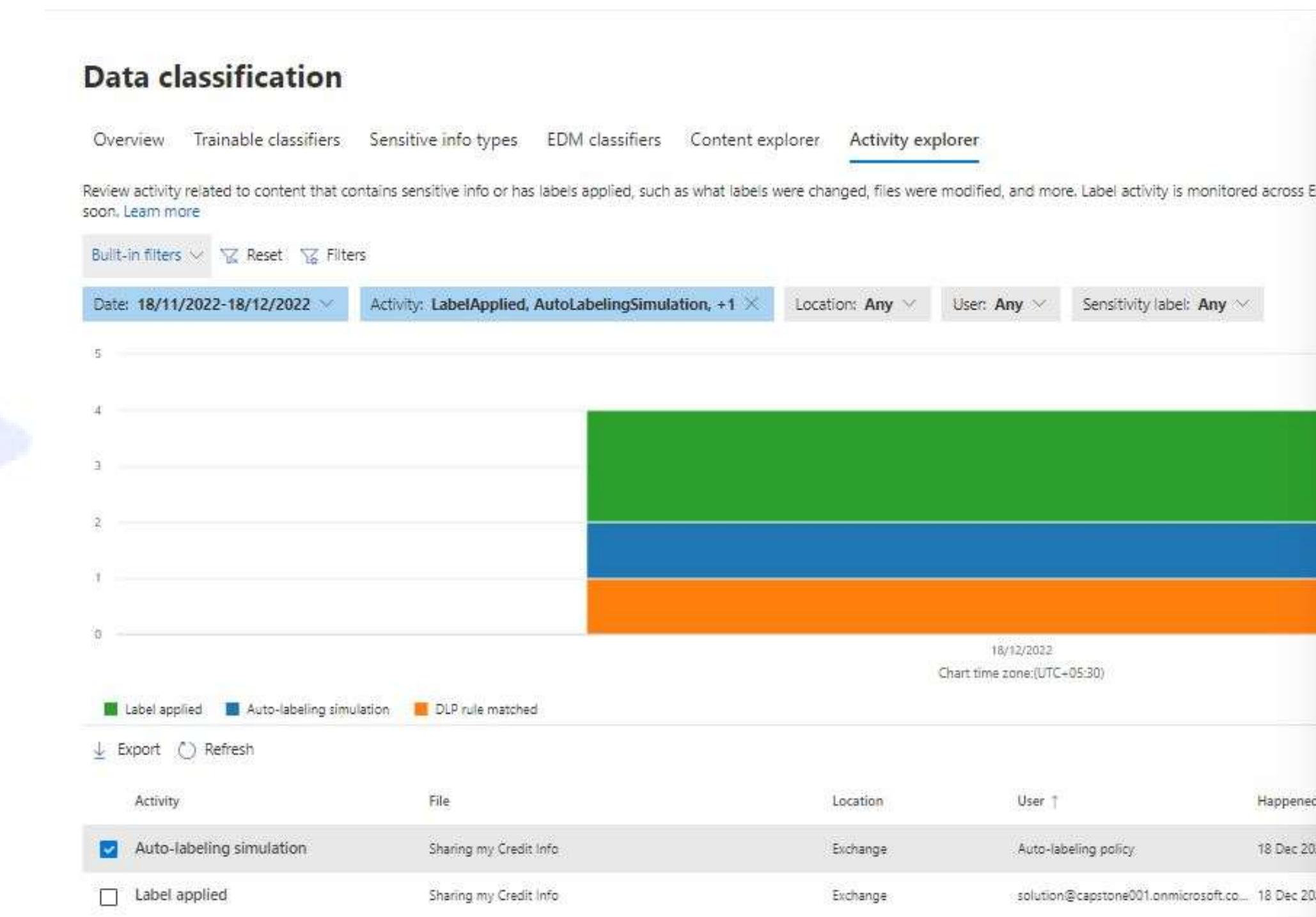




Tracks



- 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.



Auto-labeling simulation	
Activity details	
Activity	Happened
Auto-labeling simulation	18 Dec 2022 3:45 PM
How applied	
Auto	Label event type
	None
About this item	
File	User
Sharing my Credit Info	Auto-labeling policy
File size	Sensitivity label
24 KB	defa4170-0d19-0005-000a-bc88714345d2
Sensitive info type	Policy
Credit Card Number	PCI Data Security Standard (PCI DSS)
Rule	Policy mode
adffa528-0ebc-4d10-8ce9-8b30f021a7fc	Audit
Email subject	
Sharing my Credit Info	
Email sender	
solution@capstone001.onmicrosoft.com	



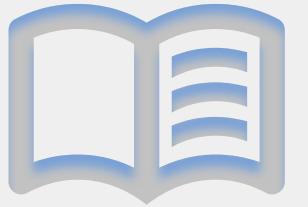
All in one



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

P.I.M REPORT
COMPLETE DLP SOLUTION

Under The Guidance:
Dr. Sibi Chakkaravarthy Sethuraman

Centre Of Excellence
Cyber Security

Team:
Tarun R - 19BCN7122
Praveen K - 19BCE7595
Nikhil V - 19BCE7130

VIT-AP
UNIVERSITY

For 100\$ only

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