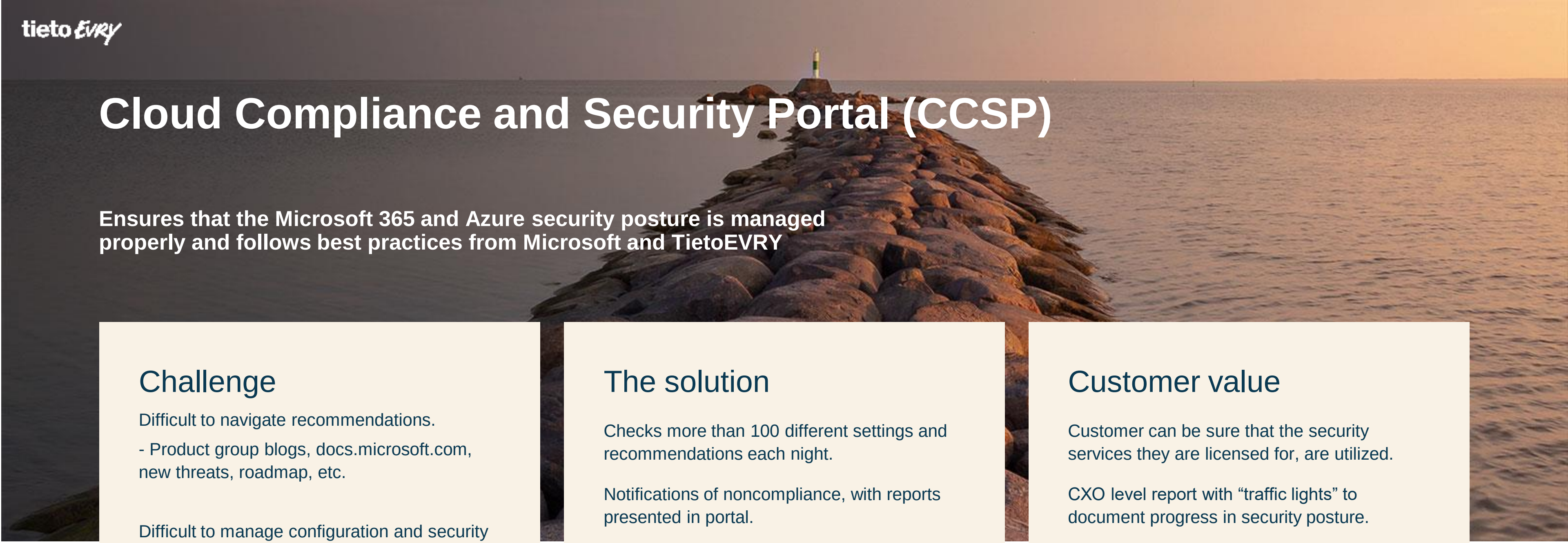
TietoEVRY Cloud Compliance and Security Portal



Cloud Compliance and Security Portal (CCSP)

Ensures that the Microsoft 365 and Azure security posture is managed properly and follows best practices from Microsoft and TietoEVRY

Challenge

Difficult to navigate recommendations.

- Product group blogs, docs.microsoft.com, new threats, roadmap, etc.

Difficult to manage configuration and security baseline drift.

Constant flow of new recommendations and features.

Difficult to have overview of service principals and privileged access.

The solution

Checks more than 100 different settings and recommendations each night.

Notifications of noncompliance, with reports presented in portal.

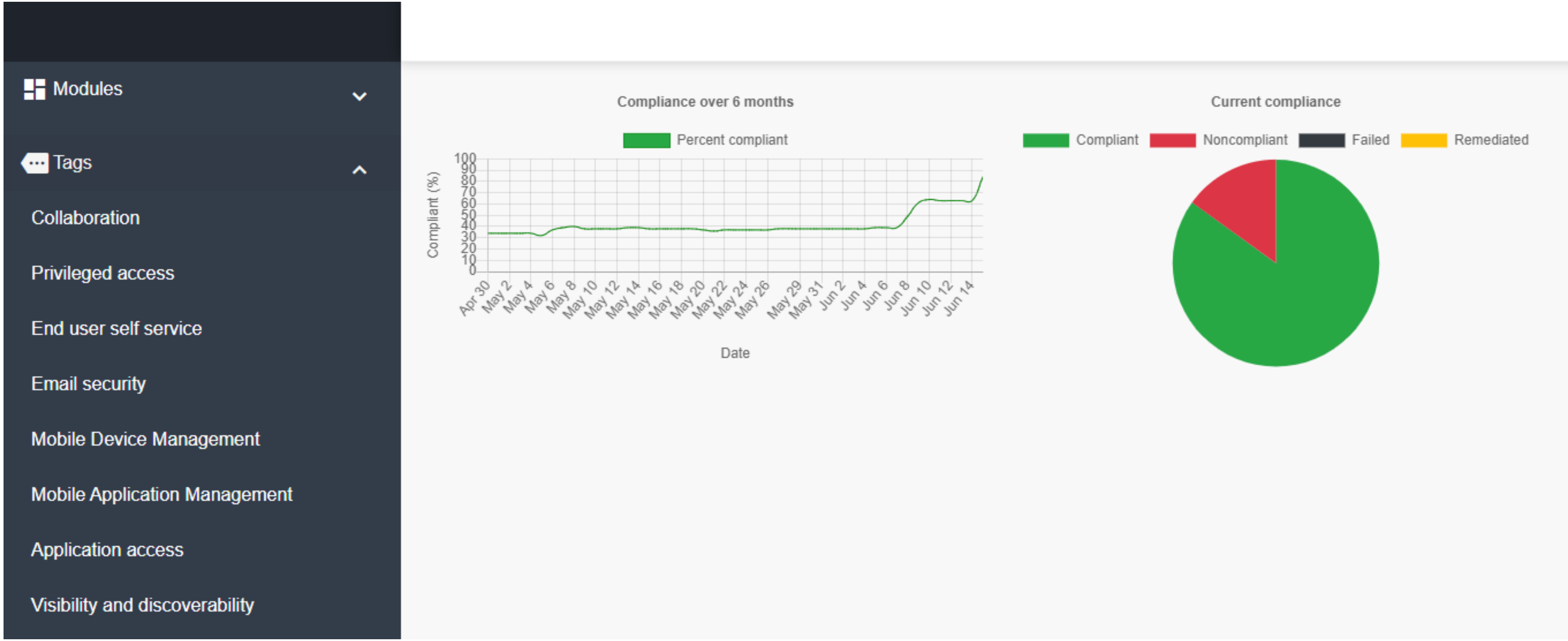
Detailed instructions on «Why this policy?», «How to remediate?» and «How does this affect my users?».

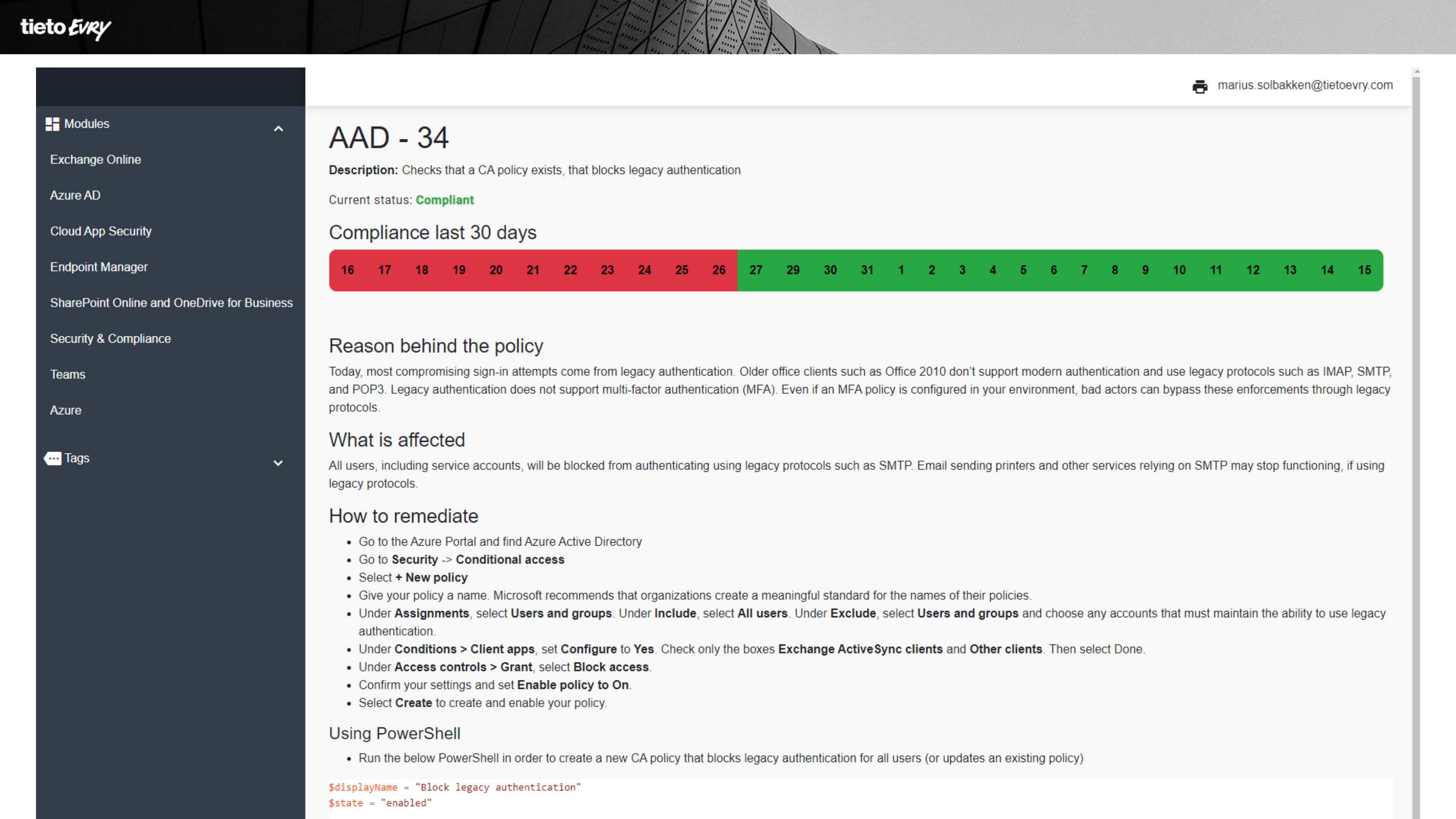
Customer value

Customer can be sure that the security services they are licensed for, are utilized.

CXO level report with “traffic lights” to document progress in security posture.

One place to get recommendations for tenant.


Modules
Tags
Collaboration
Privileged access
End user self service
Email security
Mobile Device Management
Mobile Application Management
Application access
Visibility and discoverability
Compliance over 6 months
Percent compliant
100
90
80
70
60
50
40
30
20
10
0
Compliant (%)
Apr 30
May 2
May 4
May 6
May 8
May 10
May 12
May 14
May 16
May 18
May 20
May 22
May 24
May 26
May 29
May 31
Jun 2
Jun 4
Jun 6
Jun 8
Jun 10
Jun 12
Jun 14
Date
Current compliance
Compliant
Noncompliant
Failed
Remediated



AAD - 34

Description: Checks that a CA policy exists, that blocks legacy authentication

Current status: **Compliant**

Compliance last 30 days

16	17	18	19	20	21	22	23	24	25	26	27	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Reason behind the policy

Today, most compromising sign-in attempts come from legacy authentication. Older office clients such as Office 2010 don't support modern authentication and use legacy protocols such as IMAP, SMTP, and POP3. Legacy authentication does not support multi-factor authentication (MFA). Even if an MFA policy is configured in your environment, bad actors can bypass these enforcements through legacy protocols.

What is affected

All users, including service accounts, will be blocked from authenticating using legacy protocols such as SMTP. Email sending printers and other services relying on SMTP may stop functioning, if using legacy protocols.

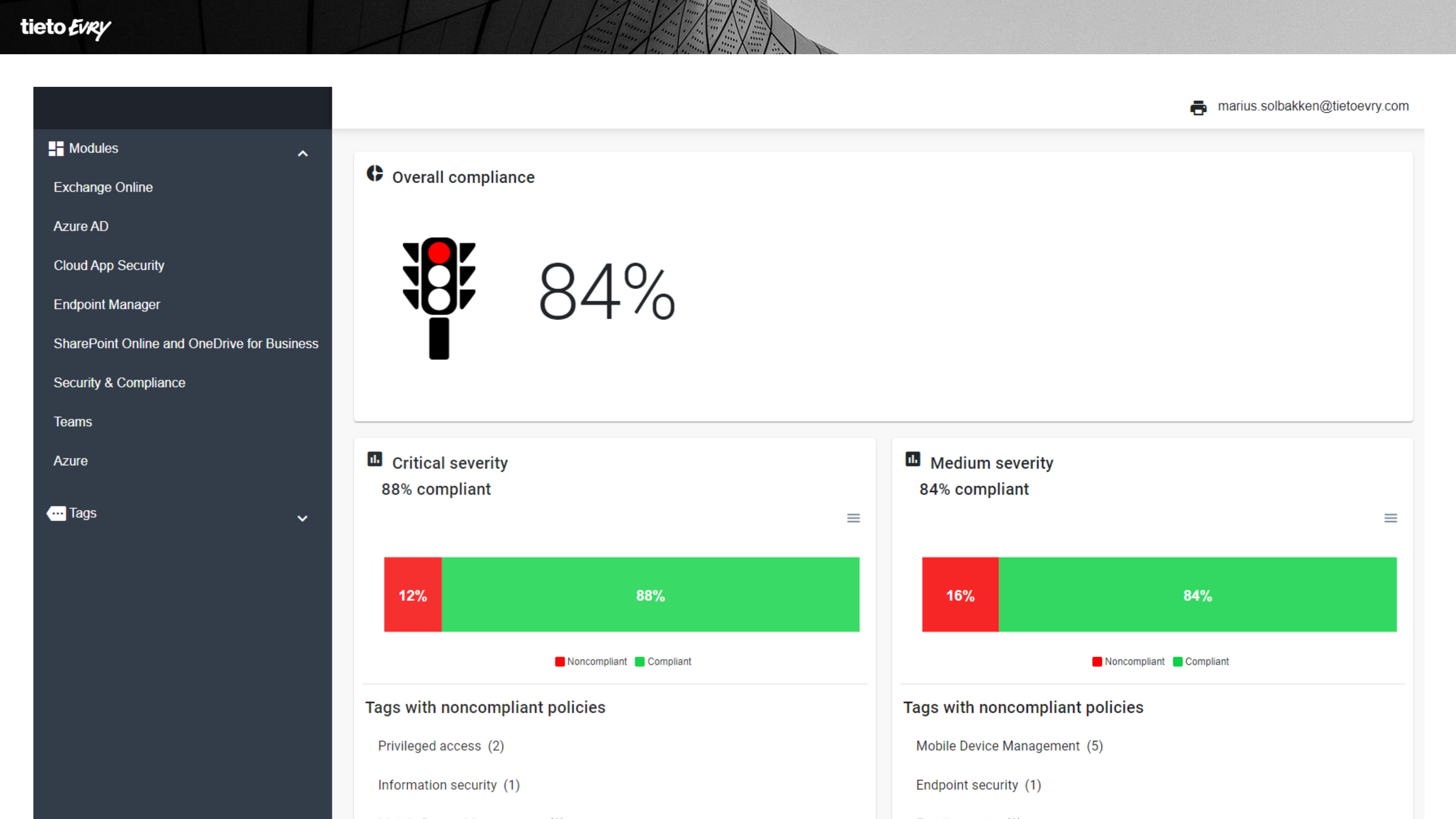
How to remediate

- Go to the Azure Portal and find Azure Active Directory
- Go to **Security** -> **Conditional access**
- Select **+ New policy**
- Give your policy a name. Microsoft recommends that organizations create a meaningful standard for the names of their policies.
- Under **Assignments**, select **Users and groups**. Under **Include**, select **All users**. Under **Exclude**, select **Users and groups** and choose any accounts that must maintain the ability to use legacy authentication.
- Under **Conditions > Client apps**, set **Configure** to **Yes**. Check only the boxes **Exchange ActiveSync clients** and **Other clients**. Then select Done.
- Under **Access controls > Grant**, select **Block access**.
- Confirm your settings and set **Enable policy to On**.
- Select **Create** to create and enable your policy.

Using PowerShell

- Run the below PowerShell in order to create a new CA policy that blocks legacy authentication for all users (or updates an existing policy)

```
$displayName = "Block legacy authentication"
$state = "enabled"
```


tieto EVRY
marius.solbakken@tietoevry.com
Modules
Exchange Online
Azure AD
Cloud App Security
Endpoint Manager
SharePoint Online and OneDrive for Business
Security & Compliance
Teams
Azure
Tags

Overall compliance

84%

Critical severity

88% compliant

12%
88%
🟥 Noncompliant 🟩 Compliant

Tags with noncompliant policies

Privileged access (2)

Information security (1)

Medium severity

84% compliant

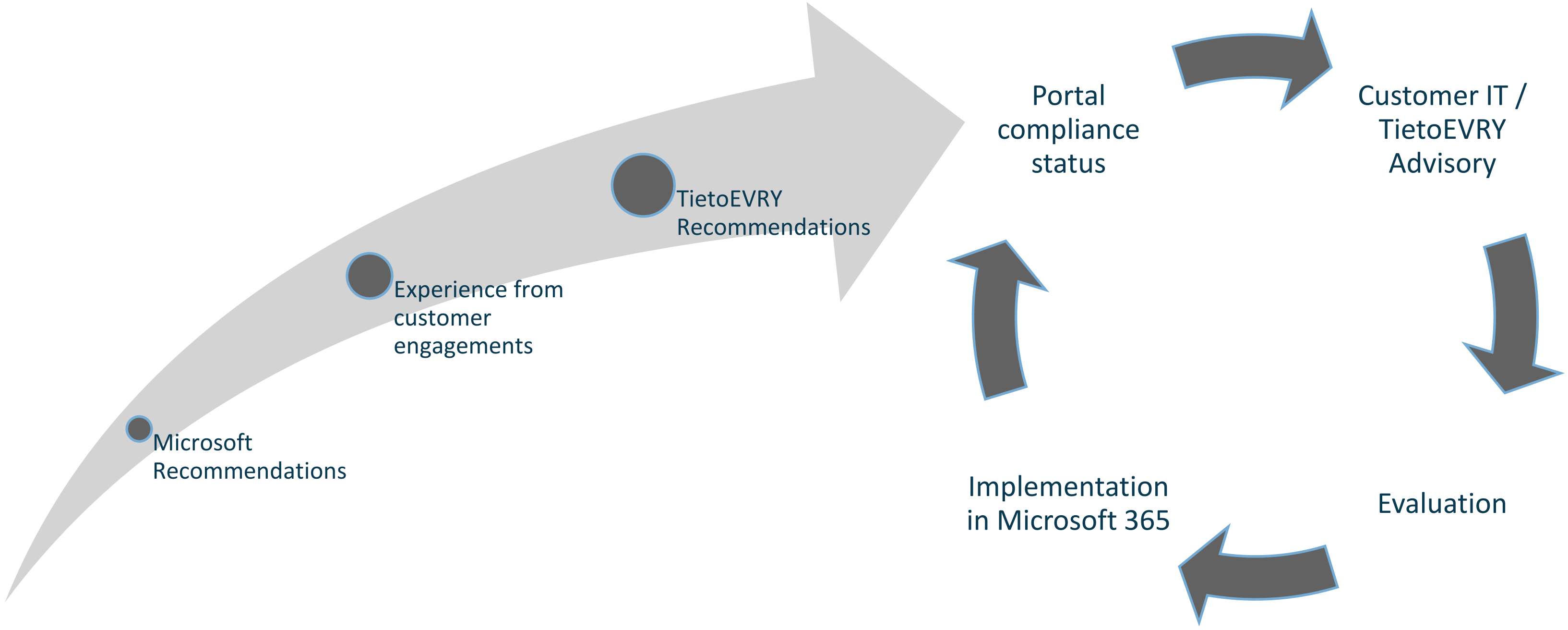
16%
84%
🟥 Noncompliant 🟩 Compliant

Tags with noncompliant policies

Mobile Device Management (5)

Endpoint security (1)

Process



Microsoft Recommendations
Experience from customer engagements
TietoEVRY Recommendations
Portal compliance status
Customer IT / TietoEVRY Advisory
Evaluation
Implementation in Microsoft 365

What permissions are needed by the service?

- Consent to application with delegated permissions only
- Reader on Azure Subscriptions
- MCAS API read only token
- User account with
    - Global Reader
    - Security Reader
    - Authentication Policy Administrator (Required in order to read certain things not currently provided by Global Reader)
    - SharePoint Administrator (Required in order to access SharePoint Online PowerShell)

Where is the service running?

- Azure native service, built with Azure PaaS services running in customer preferred Azure data center (West Europe by default)
- Running in an Azure subscription in a tenant managed by Public Cloud Norway, TietoEVRY