

SERVICE DOCUMENTATION

SHADOW IT OVERSIGHT

Take stock of SaaS apps:

- IT-Approved Apps
- Non-IT-Approved Apps

Description:

- IT-Approved-Apps: SaaS apps set up and maintained by the IT team with security attributes such as SSO enablement, Azure AD group assignment and User Restrictions.
- Non-IT-Approved Apps: SaaS apps which users connect to the organization's SaaS ecosystem themselves, for personal use or to enhance business value for their unit. A user can approve risky app access in two ways:
 - Clicking a "Sign up with Microsoft" button
 - Signing up with the app then approving access via OAuth consent

Risks:

- Statistically, 77% of apps are managed by business teams without direct IT involvement. They may lack security attributes such as MFA, SSO Enablement to protect them.
- Duplicate SaaS subscriptions not only distribute data further, they also lead to cost wastage. For example: multiple CRM solutions, multiple instances of the same apps spread among different business teams.
- Malicious third-party SaaS application risk is on the rise. Attackers are adding malicious applications to app stores and marketplaces every day in an attempt to compromise high value targets.

Recommendations:

- Take stock of IT-Approved Apps and Non-IT-Approved Apps.
 - Elevate Non-IT-Approved Apps with high degrees of penetration to IT-Approved apps with the right security attributes.
 - Disable Risky Non-IT-Approved Apps and reduce attack surface
 - Identify duplicates and consolidate subscriptions.
-

PRIVILEGED ACCESS OVERSIGHT

Who's got what level of access privileges to SaaS apps?

- Highly Privileged Users
- Privileged Users

Description:

- **Highly Privileged Users** with the highest level of administrative privileges such as modifying, adding, deleting settings, data and users.
- **Privileged Users:** users with some degree of administrative privileges such as resetting passwords for users and managing certain features.

Risks:

- If privileges are misused either by accident or with malicious intent, Highly Privileged Users can cause significant damage to the SaaS solution and even the organization.
- Similar to Highly Privileged Users, Privileged Users can pose considerably larger risk than non-privileged users due to their elevated capabilities and access
- Detecting Drift in Highly Privileged Users and Privileged Users not only mitigates data breach risks, it also provides evidence of privileged access oversight, a compliance requirement for regulated entities, their vendors and suppliers.

Recommendations:

- Keep Highly Privileged Users and Privileged Users to fewer than 5 respectively per SaaS solution to minimize excessive privilege risks.
 - Set up alert notifications for privileged access Drift.
-

ACCESS OVERSIGHT

Who's got access to which SaaS apps?

- Users
- External Users
- Ghost Users
- Inactive Users

Description:

- **Users:** users who have access but who are not Highly Privileged Users or Privileged Users.
- **External Users:** users whose email addresses do not belong to the organization's internal domains.
- **Ghost Users:** users who have been disabled or deleted in the organization's identity provider such as Office 365, G Suite, OKTA, but are still enabled in other SaaS platforms.
- **Inactive Users:** accounts which have not been logged in 60 days or longer.

Risks:

- External or guest accounts may have access to the organization's business critical and customer sensitive data. They often reuse passwords and frequently are not in scope for controls such as MFA. External users may not have sufficient

(or any) contractual liabilities to the organization, in the event of breach there may be zero recourse even if negligence can be proved.

- Ghost Users not only can log in SaaS platforms undetected, their licenses are also being paid for. This costs money and gives rise to data theft risk.
- Inactive Users not only cost money, they also increase data theft risk.

Recommendations:

- Review and minimize the presence of external users. Evaluate the privileges of all external users, reduce or remove any access that is not required based on business need and last use. Remove if not required anymore. Implement an external users process in each SaaS solution.
- Review Ghost Users, remove their administrative privileges (if applicable) and disable these users in the platforms they can still access.
- Review Inactive Users especially those with access to the organizations' business critical and customer sensitive data. Evaluate the privileges of these users, reduce or remove any access that is not required based on business need and last use. Remove if not required anymore.

AUTHENTICATION OVERSIGHT

Which users are not logging in securely?

- Disabled MFA
- Non-Federated

Description:

- **Disabled MFA:** accounts whose MFA status is disabled or unenforced.

- **Non-Federated:** accounts not federated to the organization's identity provider such as Office 365, G Suite, OKTA.

Risks:

- MFA is widely regarded as the most effective control in preventing Business Email Compromise & Password Reuse attacks. Microsoft states that MFA can block over 99.9 percent of account compromise attacks. The risk of these attacks is much larger when the compromised account is either a Highly Privileged or Privileged User due to their authorization to access systems, data, users and make changes.
- Non-Federated accounts pose a significant security risk to SaaS solutions holding business critical and customer sensitive data. They will often be missed in privileged user audits, have credentials rotated or removed by user offboarding processes.

Recommendations:

- Enforce MFA for all users at all times.
- Enforce federation for all accounts.

DATA PROTECTION OVERSIGHT

Who's sharing data with whom?

- External Mail Forward
- Internal Mail Forward
- External Shares
- DLP Events

Description:

- External Mail Forward: rules created by users to automatically forward their

emails to external domain email addresses.

- Internal Mail Forward: rules created by users to automatically forward their emails to other internal email addresses.
- External Shares: externally shared drives and files.
- DLP Events: Data Loss Prevention events triggered in line with default or custom policies set by your organization in the SaaS solution.

Risks:

- Auto-forward rules are often used by cybercriminals in business email compromise attacks. The risk of these attacks is much larger when the compromised account belongs to a Highly Privileged User or Privileged User due to their authorization to access systems, data, users and make changes.
- While sharing and co-editing documents are powerful tools being harnessed by modern workplaces, it is critical to have visibility of external sharing to confirm that oversharing has not happened. Examples of oversharing accidentally sharing an entire folder instead of a file, edit rights were granted instead of read-only, the external party re-shared the file with a different external party.
- DLP Events can lead to unintentional or accidental exposure of sensitive information to unwanted parties, a leading cause of cyber breaches.

Recommendations:

- Review for signs of malicious activity and remove all malicious or unnecessary External and Internal Mail Forward rules. Conduct Cyber Awareness training with staff around the dangers of auto-forward rules.
- Review all documents that are shared publicly. Remove sharing on any that would be considered sensitive. Undertake a cyber education uplift with the staff who have enabled link sharing on sensitive documents around appropriate

handling of data. Investigate if using information classification and tagging content is appropriate for your organization.

- Investigate the most recent events to confirm that no immediate DLP Events are ongoing. Conduct a cyber education / awareness campaign to educate staff on appropriate data handling.
-

SHADOW IT OVERSIGHT

Take stock of SaaS apps:

- IT-Approved Apps
- Non-IT-Approved Apps
- Permissions to Data

Description:

- **IT-Approved-Apps:** SaaS apps set up and maintained by the IT team with security attributes such as SSO enablement, Azure AD group assignment and User Restrictions.
- **Non-IT-Approved Apps:** SaaS apps which users connect to the organization's SaaS ecosystem themselves, for personal use or to enhance business value for their unit. A user can approve risky app access in two ways:
 - Clicking a "Sign up with Microsoft" button
 - Signing up with the app then approving access via OAuth consent

Risks:

- Statistically, 77% of apps are managed by business teams without direct IT involvement. They may lack security attributes such as MFA, SSO Enablement to

protect them.

- Duplicate SaaS subscriptions not only distribute data further, they also lead to cost wastage. For example: multiple CRM solutions, multiple instances of the same apps spread among different business teams.
- Malicious third-party SaaS application risk is on the rise. Attackers are adding malicious applications to app stores and marketplaces every day in an attempt to compromise high value targets.

Recommendations:

- Take stock of IT-Approved Apps and Non-IT-Approved Apps.
 - Elevate Non-IT-Approved Apps with high degrees of penetration to IT-Approved apps with the right security attributes.
 - Disable Risky Non-IT-Approved Apps and reduce attack surface
 - Identify duplicates and consolidate subscriptions.
 - Evaluate if marketplace and OAuth federations should be enabled or disabled in SaaS solutions containing business critical and customer sensitive data.
-

3RD PARTY APP INTEGRATION OVERSIGHT

Are there third-party apps accessing data?

Description:

- Third-Party App Integrations: normally done by way of SaaS marketplace integrations: a privileged user authorizes a third-party application published in the SaaS marketplace to access or copy data between SaaS solutions.


Risks:

- Malicious third-party SaaS application risk is on the rise. Attackers are adding malicious applications to app stores and marketplaces every day in an attempt to

compromise high value targets.

Recommendations:

- Review all currently authorized applications on SaaS solutions, both via marketplaces and OAuth.
- Evaluate if marketplace and OAuth federations should be enabled or disabled in SaaS solutions containing business critical and customer sensitive data.

SaaS	PRIVILEGED ACCESS OVERSIGHT		USER ACCESS OVERSIGHT				AUTHENTICATION OVERSIGHT		BUSINESS EMAIL OVERSIGHT		DATA PROTECTION OVERSIGHT		
	Highly Privileged Users	Privileged Users	Users	External Users	Ghost Users	Inactive Users	MFA	Identity Federation	External Mail Forward	Internal Mail Forward	External Shares	DLP Events	3rd Party App Integrations
	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A
	✓	✓	✓	✓	✓	✓	N/A	✓	N/A	N/A	✓	N/A	N/A
	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A
	✓	✓	✓	✓	✓	N/A	✓	N/A	N/A	N/A	N/A	N/A	N/A
	✓	✓	✓	✓	✓	N/A	✓	N/A	N/A	N/A	N/A	N/A	N/A
	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	✓	N/A	Coming soon
	✓	✓	✓	✓	✓	N/A	✓	N/A	N/A	N/A	N/A	N/A	N/A
	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	✓	N/A	N/A
	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	✓	N/A	N/A