Summary

[SaaS Security Controls Checklist (Based on MITRE ATT&CK for SaaS) 1](#_Toc207271044)

[Reconnaissance 1](#_Toc207271045)

[Initial Access 1](#_Toc207271046)

[Persistence 2](#_Toc207271047)

[Discovery 2](#_Toc207271048)

[Privilege Escalation 2](#_Toc207271049)

[Actions on Objectives / Impact 2](#_Toc207271050)

[Summary Techniques 3](#_Toc207271051)

# SaaS Security Controls Checklist based on MITRE ATT&CK for SaaS[[1]](#footnote-1)

This checklist maps MITRE ATT&CK for SaaS tactics and techniques to practical security controls that can be applied to SaaS applications.

## Reconnaissance

* Monitor for exposed employee/administrator credentials via breach-monitoring services.
* Limit publicly visible admin/user metadata (e.g., LinkedIn, GitHub).
* Implement credential rotation and enforce strong password hygiene.

## Initial Access

* Enforce phishing-resistant MFA (hardware tokens, mobile push).
* Disable or tightly control self-service password reset flows.
* Train helpdesk to follow strong verification protocols; log all password resets.
* Apply URL filtering or safe browsing tools to block malicious links.

## Persistence

* Alert and review new MFA device registrations.
* Monitor and restrict changes to access policies or creation of inbox rules.
* Enable logging for deletion of security notifications or audit trails.
* Block unwanted forwarding/automatic rules in email.

## Discovery

* Restrict access to SSO dashboards only to those who need it.
* Log and monitor searches or access to password policy documentation.
* Implement restrictions on access to sensitive IT documentation.
* Review trust relationships (like federated identity providers).

## Privilege Escalation

* Use role-based access control (RBAC) with least privilege enforcement.
* Monitor API usage (e.g., MS Graph) for anomalous behavior.
* Validate external domains aren’t added to federation trusts without authorization.
* Examine internal messaging flows for suspicious lateral movement patterns.

## Actions on Objectives / Impact

* Monitor for large-scale data downloads or downloads from uncommon locations.
* Track connections via VPNs, RDP sessions, or unusual network paths.
* Implement data encryption and data loss prevention (DLP) controls.
* Enable anomaly-based alerting for sudden changes in user behavior (e.g., high-volume file changes).

# Summary Techniques

| ATT&CK Phase | Security Controls (Checklist) |
| --- | --- |
| Reconnaissance | Monitor for exposed employee/administrator credentials via breach-monitoring services. Limit publicly visible admin/user metadata (e.g., LinkedIn, GitHub). Implement credential rotation and enforce strong password hygiene. |
| Initial Access | Enforce phishing-resistant MFA (hardware tokens, mobile push). Disable or tightly control self-service password reset flows. Train helpdesk to follow strong verification protocols; log all password resets. Apply URL filtering or safe browsing tools to block malicious links. |
| Persistence | Alert and review new MFA device registrations. Monitor and restrict changes to access policies or creation of inbox rules. Enable logging for deletion of security notifications or audit trails. Block unwanted forwarding/automatic rules in email. |
| Discovery | Restrict access to SSO dashboards only to those who need it. Log and monitor searches or access to password policy documentation. Implement restrictions on access to sensitive IT documentation. Review trust relationships (like federated identity providers). |
| Privilege Escalation | Use role-based access control (RBAC) with least privilege enforcement. Monitor API usage (e.g., MS Graph) for anomalous behavior. Validate external domains aren’t added to federation trusts without authorization. Examine internal messaging flows for suspicious lateral movement patterns. |
| Actions on Objectives / Impact | Monitor for large-scale data downloads or downloads from uncommon locations. Track connections via VPNs, RDP sessions, or unusual network paths. Implement data encryption and data loss prevention (DLP) controls. Enable anomaly-based alerting for sudden changes in user behavior (e.g., high-volume file changes). |

1. <https://attack.mitre.org/matrices/enterprise/cloud/saas> [↑](#footnote-ref-1)