

SaaS Posture Findings Report

Services: All Services

Tenants: All Tenants














Include: All existing rules and settings

Generated: Feb 28, 2025 20:16 UTC

Created by: [Ryusei Kent](#)

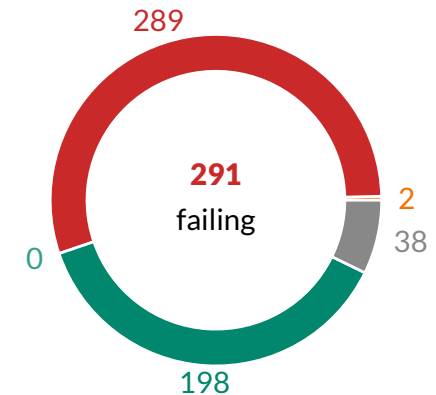
Organization: [tevo](#)

Posture status by service

Service	Failing	Failing but accepted	Passing with	Passing	Other
 Atlassian	15	—	—	7	—
 Cloudflare	5	—	—	1	—
 Datadog	7	—	—	10	—
 GitHub	5	2	—	19	—
 Google	9	—	—	6	25
 HubSpot	1	—	—	2	—
 Jamf	4	—	—	4	—
 Microsoft	149	—	—	107	7
 Okta	26	—	—	21	5
 SendGrid	3	—	—	—	—
 Slack	7	—	—	2	—
 Snowflake	31	—	—	3	1
 Zoom	27	—	—	16	—
Total	289	2	—	198	38

















Summary

230 rules and 297 settings



- Failing but accepted 0.4%
- Failing 54.8%
- Passing with exceptions 0.0%
- Passing 37.6%
- Other 7.2%

Posture status by tenant

Tenant	Failing	Failing but accepted	Passing with	Passing	Other
 Atlassian Admin2	15	—	—	7	—
 Logitix - Cloudflare	5	—	—	1	—
 Datadog	7	—	—	10	—
 GitHub	2	2	—	9	—
 GitHub 1T	3	—	—	10	—
 Google Workspace	7	—	—	1	25
 Google Workspace_DTI_Mar	2	—	—	5	—
 HubSpot	1	—	—	2	—
 Jamf Pro	4	—	—	4	—
 Microsoft Graph - Azure AD	79	—	—	57	3
 Victory Live - Microsoft Graph	70	—	—	50	4
 Okta	26	—	—	21	5
 Sendgrid	3	—	—	—	—
 Victory Live Slack	7	—	—	2	—
 Logitix - Snowflake	31	—	—	3	1
 Victory Live - Zoom	27	—	—	16	—
Total	289	2	—	198	38

Posture Rules

5 Failing, 7 Passing

Rule	Risk	State	Violations	Exceptions
Confluence external privileged users	High	Passing	—	—
Confluence privileged users with a low reputation domain	High	Passing	—	—
Jira privileged users with a low reputation domain	High	Passing	—	—
Jira inactive privileged accounts	Medium	Passing	—	—
Confluence inactive privileged accounts	Medium	Failing	6	—
Inactive accounts	Medium	Failing	759	—
Products with no IP allowlists	Medium	Failing	1	—
Confluence external users	Low	Passing	—	—
Confluence users with a low reputation domain	Low	Passing	—	—
Unverified added domains	Low	Passing	—	—
Data residency policies	Low	Failing	3	—
Jira users with a low reputation domain	Low	Failing	1	—

Security Related Posture Settings

10 Failing, 0 Passing

Setting	Risk	State	Value	Target
Block compromised devices	Critical	Failing	null	= true
Disable sharing, saving or backing up content from the mobile app	High	Failing	null	= true
Mobile app policy	High	Failing	null	= true
Override any IP allowlists to allow access from Jira and Conflue...	High	Failing	null	= false
Require biometric authentication or a device passcode	High	Failing	null	= true
Require data encryption	High	Failing	null	= true
Android	Medium	Failing	null	>= 33
Disable cutting or copying content from the mobile app	Medium	Failing	null	= true

Setting	Risk	State	Value	Target
Disable screenshots and screen recording of the mobile app	Medium	Failing	null	= true
iOS / iPadOS	Medium	Failing	null	>= 16

Posture Rules

4 Failing, 1 Passing

Rule	Risk	State	Violations	Exceptions
Administrator role members without MFA enabled	High	Failing	13	—
Inactive Administrator role members	High	Failing	10	—
Super Administrators	High	Failing	11	—
Inactive Non-Administrator role members	Medium	Passing	—	—
Non-Administrator role members without MFA enabled	Medium	Failing	1	—

Security Related Posture Settings

1 Failing, 0 Passing

Setting	Risk	State	Value	Target
Member 2FA enforcement	High	Failing	false	= true

Posture Rules

2 Failing, 3 Passing

Rule	Risk	State	Violations	Exceptions
Admin users with MFA disabled and SAML login not required for...	High	Passing	—	—
Datadog administrator accounts	High	Passing	21	—
Ghost administrators	High	Failing	59	—
Users with MFA disabled and SAML login not required for users	Medium	Passing	—	—
Stale user invites	Low	Failing	9	—

Security Related Posture Settings

5 Failing, 7 Passing

Setting	Risk	State	Value	Target
Authenticate users with an email and password	High	Passing	false	= false
SAML - Authenticate users with a SAML 2.0 provider of your ch...	High	Passing	true	= true
SAML - IdP metadata installed	High	Passing	true	= true
SAML - Sign in strict mode enabled	High	Passing	true	= true
Authenticate users with a Google account	Medium	Passing	false	= false
SAML - Initiated sign in enabled	Medium	Passing	true	= true
SAML - Sign in metadata uploaded	Medium	Passing	true	= true
Report Management disabled	Medium	Failing	false	= true
SAML - Domains for just-in-Time provisioning	Medium	Failing		not empty
SAML - Sign in autocreate access role	Medium	Failing	st	not one of Datadog Standard Role-, Datadog Admin Role
SAML - Sign in autocreate users domains enabled	Medium	Failing	false	= true
Static public data sharing disabled	Medium	Failing	false	= true

Posture Rules

0 Failing, 2 Failing but accepted, 7 Passing

Rule	Risk	State	Violations	Exceptions
Review repositories not using secret scanning	High	Passing	—	—
Review repositories not using secret scanning push protection	High	Passing	—	—
Review organization members with MFA disabled	Medium	Passing	—	—
Review organization outside collaborators with MFA disabled	Medium	Passing	—	—
Review organization secrets visible to a mixture of public and...	Medium	Passing	—	—
Review outside collaborators with repository admin privileges	Medium	Passing	—	—
Review outside collaborators with repository maintain privileges	Medium	Passing	—	—
Review organization secrets visible to all organization repositor...	Medium	Failing but accepted	3	—
Review site admin accounts without a verified email address	Medium	Failing but accepted	2	—

Security Related Posture Settings

2 Failing, 2 Passing

Setting	Risk	State	Value	Target
Require multi-factor authentication	High	Passing	true	= true
Organization IP whitelist in place	High	Failing	false	= true
Organization IP whitelist in place for applications	High	Failing	false	= true
Organization members can create public repositories	Medium	Passing	false	= false

Posture Rules

1 Failing, 8 Passing

Rule	Risk	State	Violations	Exceptions
Review repositories not using secret scanning	High	Passing	—	—
Review repositories not using secret scanning push protection	High	Passing	—	—
Review organization members with MFA disabled	Medium	Passing	—	—
Review organization outside collaborators with MFA disabled	Medium	Passing	—	—
Review organization secrets visible to a mixture of public and...	Medium	Passing	—	—
Review organization secrets visible to all organization repositor...	Medium	Passing	—	—
Review outside collaborators with repository admin privileges	Medium	Passing	—	—
Review outside collaborators with repository maintain privileges	Medium	Passing	—	—
Review site admin accounts without a verified email address	Medium	Failing	1	—

Security Related Posture Settings

2 Failing, 2 Passing

Setting	Risk	State	Value	Target
Require multi-factor authentication	High	Passing	true	= true
Organization IP whitelist in place	High	Failing	false	= true
Organization IP whitelist in place for applications	High	Failing	false	= true
Organization members can create public repositories	Medium	Passing	false	= false

Posture Rules

7 Failing, 1 Passing

Rule	Risk	State	Violations	Exceptions
Org units with inbound third-party SSO disabled	High	Passing	—	—
Public and anyone with the link sensitive files	High	Failing	594	—
User logins with SMS and phone calls for MFA	High	Failing	80	—
Inactive non-privileged accounts	Medium	Failing	245	—
Inactive privileged accounts	Medium	Failing	3	—
Mailbox forwarding	Medium	Failing	131	—
Public and anyone with the link files	Medium	Failing	10215	—
Mailbox delegates	Low	Failing	60	—

Security Related Posture Settings

0 Failing, 0 Passing, 25 Other

Setting	Risk	State	Value	Target
Android device management	High	No data	null	= Advanced
Enforce password policy at next sign-in	High	No data	null	= true
Enforce strong password	High	No data	null	= true
Google Sync device management	High	No data	null	= Advanced
Less secure app access	High	No data	null	= Disable access to less secure apps
Minimum password length	High	No data	null	>= 12
Password strength	High	No data	null	= Strong
Require users to set a password	High	No data	null	= true
Set minimum characters	High	No data	null	>= 12
iOS device management	High	No data	null	= Advanced
Allow password reuse	Medium	No data	null	= false
Block compromised Android devices	Medium	No data	null	= true

Setting	Risk	State	Value	Target
Block expired passwords	Medium	No data	null	>= 2
Block jailbroken iOS devices	Medium	No data	null	= true
Device encryption requirement	Medium	No data	null	= true
Manage Google Workspace Marketplace allowlist access	Medium	No data	null	!= Allow users to install and run any app from the Marketplace
Require admin approval	Medium	No data	null	= true
Wipe device after failed attempts	Medium	No data	null	= 12
External directory sharing	Low	No data	null	= Authenticated user basic profile fields
Manage Google Workspace Marketplace internal app access	Low	No data	null	= true
Maximum password length	Low	No data	null	>= 100
Password lifespan	Low	No data	null	<= 100
Password reset frequency	Low	No data	null	!= Never expires
Send monthly report of inactive company owned devices to super...	Low	No data	null	= true
Set time until screen locks	Low	No data	null	<= 180

Posture Rules

2 Failing, 5 Passing

Rule	Risk	State	Violations	Exceptions
Public and anyone with the link sensitive files	High	Passing	—	—
User logins with SMS and phone calls for MFA	High	Passing	—	—
Inactive non-privileged accounts	Medium	Passing	—	—
Inactive privileged accounts	Medium	Passing	—	—
Mailbox forwarding	Medium	Failing	5	—
Public and anyone with the link files	Medium	Failing	3	—
Mailbox delegates	Low	Passing	—	—

Security Related Posture Settings

No existing settings

Posture Rules

1 Failing, 2 Passing

Rule	Risk	State	Violations	Exceptions
Sensitive files with non-private visibility	High	Passing	—	—
Super administrator accounts	High	Failing	12	—
Databases with public API access	Medium	Passing	—	—

Security Related Posture Settings

No existing settings

Posture Rules

3 Failing, 3 Passing

Rule	Risk	State	Violations	Exceptions
Ghost administrators	High	Passing	—	—
Users with ability to remotely wipe or lock devices	High	Passing	—	—
Accounts with administrator privileges	High	Failing	8	—
Users with Sensitive Device Management Privileges	Medium	Passing	—	—
Accounts with full access	Medium	Failing	9	—
Jamf Pro users from external domains	Medium	Failing	9	—

Security Related Posture Settings

1 Failing, 1 Passing

Setting	Risk	State	Value	Target
Enable SSO	Critical	Failing	false	= true
SSO Bypass Allowed	High	Passing	false	= false

Posture Rules

32 Failing, 21 Passing

Rule	Risk	State	Violations	Exceptions
Domains with any.sts backdoor	Critical	Passing	—	—
User logins using legacy authentication protocols in the last 14...	Critical	Passing	—	—
Admins without MFA registered	Critical	Failing	4	—
External privileged users	Critical	Failing	3	—
Global administrators	Critical	Failing	16	—
Azure Devops projects that allow fork builds access to secrets	High	Passing	—	—
Domains with an unusual validity period in signing certificates	High	Passing	—	—
Domains with signing certificate mismatch	High	Passing	—	—
High privileged service principals with credentials	High	Passing	—	—
Intune administrator accounts	High	Passing	—	—
Mailboxes that give access to Default or Anonymous users	High	Passing	—	—
Microsoft owned application service principals with credentials	High	Passing	—	—
Misconfigured conditional access policy for MFA registration	High	Passing	—	—
Privileged Azure DevOps accounts	High	Passing	—	—
Privileged Power Platform accounts	High	Passing	—	—
Users with privileged Dynamics 365 access	High	Passing	—	—
Azure Devops projects that allow any variables to be set at queue...	High	Failing	22	—
Azure Devops projects that allow building pull requests from fo...	High	Failing	43	—
Azure Devops projects that allow unsanitized shell task argume...	High	Failing	48	—
Inactive privileged accounts	High	Failing	8	—
Long-lasting personal access tokens	High	Failing	198	—
Malware filter policy with file filter disabled	High	Failing	1	—
No conditional access policy for MFA registration	High	Failing	1	—
Personal access token with full access	High	Failing	16	—
Users with ApplicationImpersonation Exchange role	High	Failing	4	—

Rule	Risk	State	Violations	Exceptions
Users with privileged Sharepoint access	High	Failing	8	—
Users without MFA registered	High	Failing	408	—
Users without SearchQueryInitiated activated	High	Failing	13	—
Azure Devops projects that allow forked GitHub repositories to...	Medium	Passing	—	—
Calendar sharing policy with other Exchange organizations	Medium	Passing	—	—
Conditional access policy with persistent browser	Medium	Passing	—	—
Safe attachment policy action	Medium	Passing	—	—
Spoof intelligence not enabled in anti-phish policy	Medium	Passing	—	—
Users with advanced auditing disabled	Medium	Passing	—	—
Azure Devops projects that allow pipeline to access non-refere...	Medium	Failing	25	—
Azure Devops projects that do not limit authorization in non-rel...	Medium	Failing	22	—
Azure Devops projects that do not limit authorizations in release...	Medium	Failing	35	—
DomainKeys Identified Mail signing configuration disabled	Medium	Failing	7	—
Inactive non-privileged accounts	Medium	Failing	331	—
Mailbox intelligence not enabled in anti-phish policy	Medium	Failing	1	—
Outlook mailbox forwarding	Medium	Failing	93	—
Public groups in Microsoft 365	Medium	Failing	12	—
Shared mailbox service accounts that allow sign-ins	Medium	Failing	153	—
Unverified Domains	Medium	Failing	1	—
Users from low reputation domains	Medium	Failing	21	—
Azure Devops projects that do not require comments before bu...	Low	Passing	—	—
Safe attachment policy quarantine tag	Low	Passing	—	—
Administrator is not set to be notified of outbound spam in outb...	Low	Failing	3	—
Administrator is not set to have BCC of outbound spam in outbo...	Low	Failing	3	—
Conditional access policy with sign in frequency	Low	Failing	2	—
Malware filter policy without notifications for internal users sen...	Low	Failing	1	—
Phish threshold level lower than 2	Low	Failing	2	—
User logins from foreign geographical locations	Low	Failing	120	—

Security Related Posture Settings

47 Failing, 36 Passing, 3 Other

Setting	Risk	State	Value	Target
Choose which external domains your users have access to	Critical	Passing	Block all external domains	= Block all external domains
Enable password protection on Windows Server Active Directory	Critical	Passing	true	= true
Modern authentication	Critical	Passing	true	= true
Apps that don't use modern authentication	Critical	Failing	true	= false
Disallow infected file download	Critical	Failing	false	= true
Allow mailbox auditing for the organization	High	Passing	false	= false
Allow people to click through Protected View even if Safe Docu...	High	Passing	false	= false
Audit log search is enabled	High	Passing	true	= true
Custom banned password lists	High	Passing	logitixlogitix1autoprocessor 12345678usernamedynastyseÅ	!=
Custom script execution is restricted on tenant site	High	Passing	Enabled	= Enabled
Enable 'Require number matching for push notifications' in Micr...	High	Passing	enabled	= enabled
Enable ATP for SharePoint, Teams, OneDrive	High	Passing	true	= true
Enable Microsoft Authenticator	High	Passing	enabled	= enabled
Enforce custom list	High	Passing	true	= true
Internal phishing protection for Microsoft Forms	High	Passing	true	= true
Turn on Safe Documents for Office clients	High	Passing	true	= true
Allow communication with Teams users that are not managed by...	High	Failing	true	= false
Password protection mode for Windows Server Active Directory	High	Failing	Audit	= Enforced
Restrict guest access permissions	High	Failing	Guest users have limited access to properties and memberships...	= Guest user access is restricted to properties and memberships of th- eir own directory objects (most re- strictive)
Restrict who can invite guests	High	Failing	everyone	one of adminsAndGuestInviters,n- one
Set passwords to never expire	High	Failing	false	= true
Folders	High	Not applicable	Edit	= View

Setting	Risk	State	Value	Target
Allow communication with Skype users that are not managed by...	Medium	Passing	false	= false
Allow users dialing in to bypass the lobby	Medium	Passing	false	= false
Choose the permission that's selected by default for sharing links	Medium	Passing	View	= View
Choose the type of link that's selected by default when users sh...	Medium	Passing	Direct	= Direct
Content pin	Medium	Passing	RequiredOutsideScheduleMeeting	= RequiredOutsideScheduleMeeting
External content sharing is restricted	Medium	Passing	ExternalUserSharingOnly	!= ExternalUserAndGuestSharing
Group excluded in 'Show application name in push and passwor...	Medium	Passing	No group	= No group
Group excluded in 'Show geographic location in push and passw...	Medium	Passing	No group	= No group
Group included in 'Require number matching for push notificati...	Medium	Passing	all_users	= all_users
Group included in 'Show application name in push and passwor...	Medium	Passing	all_users	= all_users
Group included in 'Show geographic location in push and passw...	Medium	Passing	all_users	= all_users
IP Address Enforcement	Medium	Passing	false	= false
Meeting end to end encryption	Medium	Passing	DisabledUserOverride	= DisabledUserOverride
Sign out after	Medium	Passing	0	<= 30
Allow guest to share items they don't own	Medium	Failing	true	= false
Allow guest user	Medium	Failing	true	= false
Calendar - External sharing	Medium	Failing	true	= false
Enable 'Show application name in push and passwordless notific...	Medium	Failing	default	= enabled
Enable 'Show geographic location in push and passwordless not...	Medium	Failing	default	= enabled
Enable integration for SharePoint with Azure AD B2B	Medium	Failing	false	= true
External users with Teams accounts not managed by an organiz...	Medium	Failing	true	= false
Guest access to a site or OneDrive will expire automatically	Medium	Failing	false	= true
Idle session timeout	Medium	Failing	1000000	<= 180
Is multiple data locations for services enabled	Medium	Failing	null	= false
Number of days before reauthentication	Medium	Failing	30	<= 15
Number of days that guest has access to a site or OneDrive	Medium	Failing	60	<= 30
Office Store access	Medium	Failing	true	= false
OneDrive sync is restricted for unmanaged devices	Medium	Failing	false	= true
Pin length	Medium	Failing	5	>= 6

Setting	Risk	State	Value	Target
Reauthentication with verification code is restricted	Medium	Failing	false	= true
Restrict non-admin users from creating tenants	Medium	Failing	false	= true
Security compliance notification mails	Medium	Failing		not empty
Security compliance notification phones	Medium	Failing		not empty
SharePoint external sharing is managed through domain allow/d...	Medium	Failing	null	= AllowList
Starting trials on behalf of your organization	Medium	Failing	true	= false
These links must expire within this many days	Medium	Failing	999	<= 30
Types of users that can bypass the waiting lobby	Medium	Failing	EveryoneInCompany	one of InvitedUsers,OrganizerOnly,EveryoneInCompanyExcludingGuests
User can send emails to a channel email address	Medium	Failing	true	= false
User consent for applications	Medium	Failing	Allow user consent for apps	= Allow user consent for apps from verified publishers, for selected permissions
Users can register applications	Medium	Failing	true	= false
Security defaults	Medium	No data	null	= false
Files	Medium	Not applicable	Edit	= View
Allow anonymous users to start meeting	Low	Passing	false	= false
Allow communication with external domain	Low	Passing	false	= false
Allow external participant to give/request control	Low	Passing	false	= false
Enable all tips from mail tips	Low	Passing	true	= true
Enable group metrics from mail tips	Low	Passing	true	= true
Large audience threshold for mail tips	Low	Passing	25	<= 25
Password hash sync	Low	Passing	true	= true
Resource account content access	Low	Passing	NoAccess	= NoAccess
Additional storage providers are restricted in Outlook on the web	Low	Failing	true	= false
Allow anonymous users to join meeting	Low	Failing	true	= false
Allow participant give request control	Low	Failing	true	= false
Allow private calling for guest	Low	Failing	true	= false
Box is enabled for file sharing in Teams	Low	Failing	true	= false

Setting	Risk	State	Value	Target
Calling end to end encryption enabled type	Low	Failing	Disabled	= DisabledUserOverride
Citrix is enabled for file sharing in Teams	Low	Failing	true	= false
DropBox is enabled for file sharing in Teams	Low	Failing	true	= false
Egnyte is enabled for file sharing in Teams	Low	Failing	true	= false
Email from external senders is identified	Low	Failing	false	= true
Enable external recipients tips from mail tips	Low	Failing	false	= true
Google Drive is enabled for file sharing in Teams	Low	Failing	true	= false
Type of users allowed to present	Low	Failing	EveryoneUserOverride	= OrganizerOnlyUserOverride
Type of users allowed to use chat	Low	Failing	Enabled	!= Enabled

Posture Rules

15 Failing, 27 Passing

Rule	Risk	State	Violations	Exceptions
Admins without MFA registered	Critical	Passing	—	—
Domains with any.sts backdoor	Critical	Passing	—	—
External privileged users	Critical	Passing	—	—
User logins using legacy authentication protocols in the last 14...	Critical	Passing	—	—
Global administrators	Critical	Failing	4	—
Domains with an unusual validity period in signing certificates	High	Passing	—	—
Domains with signing certificate mismatch	High	Passing	—	—
High privileged service principals with credentials	High	Passing	—	—
Intune administrator accounts	High	Passing	—	—
Mailboxes that give access to Default or Anonymous users	High	Passing	—	—
Microsoft owned application service principals with credentials	High	Passing	—	—
Misconfigured conditional access policy for MFA registration	High	Passing	—	—
Privileged Azure DevOps accounts	High	Passing	—	—
Users with ApplicationImpersonation Exchange role	High	Passing	—	—
Users with privileged Dynamics 365 access	High	Passing	—	—
Users without MFA registered	High	Passing	—	—
Inactive privileged accounts	High	Failing	4	—
Malware filter policy with file filter disabled	High	Failing	1	—
No conditional access policy for MFA registration	High	Failing	1	—
Privileged Power Platform accounts	High	Failing	1	—
Users with privileged Sharepoint access	High	Failing	3	—
Users without SearchQueryInitiated activated	High	Failing	3	—
Calendar sharing policy with other Exchange organizations	Medium	Passing	—	—
Conditional access policy with persistent browser	Medium	Passing	—	—
Outlook mailbox forwarding	Medium	Passing	—	—

Rule	Risk	State	Violations	Exceptions
Safe attachment policy action	Medium	Passing	—	—
Shared mailbox service accounts that allow sign-ins	Medium	Passing	—	—
Spoof intelligence not enabled in anti-phish policy	Medium	Passing	—	—
Unverified Domains	Medium	Passing	—	—
Users with advanced auditing disabled	Medium	Passing	—	—
DomainKeys Identified Mail signing configuration disabled	Medium	Failing	4	—
Inactive non-privileged accounts	Medium	Failing	78	—
Mailbox intelligence not enabled in anti-phish policy	Medium	Failing	1	—
Public groups in Microsoft 365	Medium	Failing	1	—
Users from low reputation domains	Medium	Failing	4	—
Conditional access policy with sign in frequency	Low	Passing	—	—
Phish threshold level lower than 2	Low	Passing	—	—
Safe attachment policy quarantine tag	Low	Passing	—	—
User logins from foreign geographical locations	Low	Passing	—	—
Administrator is not set to be notified of outbound spam in outb...	Low	Failing	1	—
Administrator is not set to have BCC of outbound spam in outbo...	Low	Failing	1	—
Malware filter policy without notifications for internal users sen...	Low	Failing	1	—

Security Related Posture Settings

55 Failing, 23 Passing, 4 Other

Setting	Risk	State	Value	Target
Modern authentication	Critical	Passing	true	= true
Apps that don't use modern authentication	Critical	Failing	true	= false
Choose which external domains your users have access to	Critical	Failing	Allow all external domains	= Block all external domains
Disallow infected file download	Critical	Failing	false	= true
Allow mailbox auditing for the organization	High	Passing	false	= false
Custom script execution is restricted on tenant site	High	Passing	Enabled	= Enabled
Enable 'Require number matching for push notifications' in Micr...	High	Passing	enabled	= enabled
Internal phishing protection for Microsoft Forms	High	Passing	true	= true

Setting	Risk	State	Value	Target
Set passwords to never expire	High	Passing	true	= true
Allow communication with Teams users that are not managed by...	High	Failing	true	= false
Audit log search is enabled	High	Failing	false	= true
Enable Microsoft Authenticator	High	Failing	disabled	= enabled
Folders	High	Failing	Edit	= View
Restrict guest access permissions	High	Failing	Guest users have limited access to properties and memberships...	= Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)
Restrict who can invite guests	High	Failing	everyone	one of adminsAndGuestInviters,none
Allow people to click through Protected View even if Safe Docu...	High	No data	null	= false
Enable ATP for SharePoint, Teams, OneDrive	High	No data	null	= true
Turn on Safe Documents for Office clients	High	No data	null	= true
Allow communication with Skype users that are not managed by...	Medium	Passing	false	= false
Allow users dialing in to bypass the lobby	Medium	Passing	false	= false
Content pin	Medium	Passing	RequiredOutsideScheduleMeeting	= RequiredOutsideScheduleMeeting
Group excluded in 'Show application name in push and passwor...	Medium	Passing	No group	= No group
Group excluded in 'Show geographic location in push and passw...	Medium	Passing	No group	= No group
Group included in 'Require number matching for push notificati...	Medium	Passing	all_users	= all_users
Group included in 'Show application name in push and passwor...	Medium	Passing	all_users	= all_users
Group included in 'Show geographic location in push and passw...	Medium	Passing	all_users	= all_users
IP Address Enforcement	Medium	Passing	false	= false
Meeting end to end encryption	Medium	Passing	DisabledUserOverride	= DisabledUserOverride
Sign out after	Medium	Passing	0	<= 30
Allow guest to share items they don't own	Medium	Failing	true	= false
Allow guest user	Medium	Failing	true	= false
Calendar - External sharing	Medium	Failing	true	= false
Choose the permission that's selected by default for sharing links	Medium	Failing	null	= View
Choose the type of link that's selected by default when users sh...	Medium	Failing	AnonymousAccess	= Direct

Setting	Risk	State	Value	Target
Enable 'Show application name in push and passwordless notific...	Medium	Failing	default	= enabled
Enable 'Show geographic location in push and passwordless not...	Medium	Failing	default	= enabled
Enable integration for SharePoint with Azure AD B2B	Medium	Failing	false	= true
External content sharing is restricted	Medium	Failing	ExternalUserAndGuestSharing	!= ExternalUserAndGuestSharing
External users with Teams accounts not managed by an organiz...	Medium	Failing	true	= false
Files	Medium	Failing	Edit	= View
Guest access to a site or OneDrive will expire automatically	Medium	Failing	false	= true
Idle session timeout	Medium	Failing	1000000	<= 180
Is multiple data locations for services enabled	Medium	Failing	null	= false
Number of days before reauthentication	Medium	Failing	30	<= 15
Number of days that guest has access to a site or OneDrive	Medium	Failing	60	<= 30
Office Store access	Medium	Failing	true	= false
OneDrive sync is restricted for unmanaged devices	Medium	Failing	false	= true
Pin length	Medium	Failing	5	>= 6
Reauthentication with verification code is restricted	Medium	Failing	false	= true
Restrict non-admin users from creating tenants	Medium	Failing	false	= true
Security compliance notification mails	Medium	Failing		not empty
Security compliance notification phones	Medium	Failing		not empty
SharePoint external sharing is managed through domain allow/d...	Medium	Failing	null	= AllowList
Starting trials on behalf of your organization	Medium	Failing	true	= false
These links must expire within this many days	Medium	Failing	999	<= 30
Types of users that can bypass the waiting lobby	Medium	Failing	EveryoneInCompany	one of InvitedUsers,OrganizerOnly,Every- oneInCompanyExcludingGuests
User can send emails to a channel email address	Medium	Failing	true	= false
User consent for applications	Medium	Failing	Allow user consent for apps	= Allow user consent for apps from verified publishers, for selected pe- rmissions
Users can register applications	Medium	Failing	true	= false
Security defaults	Medium	No data	null	= false

Setting	Risk	State	Value	Target
Allow anonymous users to start meeting	Low	Passing	false	= false
Allow external participant to give/request control	Low	Passing	false	= false
Enable all tips from mail tips	Low	Passing	true	= true
Enable group metrics from mail tips	Low	Passing	true	= true
Large audience threshold for mail tips	Low	Passing	25	<= 25
Resource account content access	Low	Passing	NoAccess	= NoAccess
Additional storage providers are restricted in Outlook on the web	Low	Failing	true	= false
Allow anonymous users to join meeting	Low	Failing	true	= false
Allow communication with external domain	Low	Failing	true	= false
Allow participant give request control	Low	Failing	true	= false
Allow private calling for guest	Low	Failing	true	= false
Box is enabled for file sharing in Teams	Low	Failing	true	= false
Calling end to end encryption enabled type	Low	Failing	Disabled	= DisabledUserOverride
Citrix is enabled for file sharing in Teams	Low	Failing	true	= false
DropBox is enabled for file sharing in Teams	Low	Failing	true	= false
Egnyte is enabled for file sharing in Teams	Low	Failing	true	= false
Email from external senders is identified	Low	Failing	false	= true
Enable external recipients tips from mail tips	Low	Failing	false	= true
Google Drive is enabled for file sharing in Teams	Low	Failing	true	= false
Password hash sync	Low	Failing	false	= true
Type of users allowed to present	Low	Failing	EveryoneUserOverride	= OrganizerOnlyUserOverride
Type of users allowed to use chat	Low	Failing	Enabled	!= Enabled

Posture Rules

17 Failing, 15 Passing

Rule	Risk	State	Violations	Exceptions
Admins with no enrolled second factors	Critical	Passing	—	—
Applications using less secure sign-on methods with secure alte...	High	Passing	—	—
OIDC Applications with wildcard redirect enabled	High	Passing	—	—
SAML applications with no sign-on assertion signing	High	Passing	—	—
Sign on policies with MFA required on new devices only	High	Passing	—	—
Admins with a weak second factor	High	Failing	3	—
Authentication policies without possession factor requirement	High	Failing	3	—
Global session policies without MFA required	High	Failing	2	—
OIDC Applications with implicit grant flow	High	Failing	1	—
Password policies with a short minimum length requirement	High	Failing	1	—
Users with no enrolled second factors	High	Failing	4	—
Authentication policies with long max session lifetime	Medium	Passing	—	—
Authenticator enrollment policies that require SMS authenticat...	Medium	Passing	—	—
Factor enrollment policies that allow SMS authentication	Medium	Passing	—	—
Factor enrollment policies with no required factors	Medium	Passing	—	—
Global session policies with long max session lifetime	Medium	Passing	—	—
Password policies with low complexity requirements	Medium	Passing	—	—
Password policies without password lockout	Medium	Passing	—	—
Applications with less secure sign-on methods	Medium	Failing	1	—
Global session policies with long session timeout	Medium	Failing	1	—
Password policies that allow common passwords	Medium	Failing	1	—
Password policies that allow using personal attributes in passw...	Medium	Failing	1	—
Review inactive admin users	Medium	Failing	2	—
User with a weak second factor	Medium	Failing	89	—
Users only covered by the default global session sign-on rule	Medium	Failing	317	—

Rule	Risk	State	Violations	Exceptions
Password policies without enforcing password history	Low	Passing	—	—
Password policies without password expiration warnings	Low	Passing	—	—
Password policies with a short minimum password reset interval	Low	Failing	1	—
Review inactive users	Low	Failing	58	—
Review super administrator accounts	Low	Failing	9	—
SAML Applications with single logout disabled	Low	Failing	7	—
Policies in Okta with zero assigned rules	Informative	Passing	—	—

Security Related Posture Settings

9 Failing, 6 Passing, 5 Other

Setting	Risk	State	Value	Target
Okta platform	High	Passing	Identity Engine	= Identity Engine
Require phishing-resistant authenticator to enroll additional au...	High	Failing	false	= true
Admin console session management	High	No data	null	= true
Enforce MFA For Admin Console	High	No data	null	= true
Enable optional email enrollment for Okta Identity Engine	Medium	Passing	false	= false
IdP my account API password	Medium	Passing	false	= false
Okta admin console maximum app session lifetime	Medium	Passing	60	<= 720
FIPS compliance	Medium	Failing	false	= true
Front-channel single logout	Medium	Failing	false	= true
Okta admin console maximum app session idle time	Medium	Failing	720	<= 15
Automatically update Okta LDAP agents	Medium	No data	null	= true
Block passkeys for FIDO2 (WebAuthn) authenticators	Medium	No data	null	= true
Network restrictions for SSWS token	Medium	No data	null	= true
IdP my account API 2FA if possible	Low	Passing	false	= false
App settings permissions for custom admin roles	Low	Failing	false	= true
Dynamic OS version compliance	Low	Failing	false	= true
Enable custom admin roles for device permissions	Low	Failing	false	= true
Enable custom admin roles for identity providers	Low	Failing	false	= true

Setting	Risk	State	Value	Target
Windows Autopilot enrollment policy	Low	Failing	false	= true
Include the sign in with FastPass button when a Smart Card ide...	Informative	Passing	false	= false

Posture Rules

No existing rules

Security Related Posture Settings

3 Failing, 0 Passing

Setting	Risk	State	Value	Target
Require TLS enabled	Medium	Failing	false	= true
Require valid cert	Medium	Failing	false	= true
Version	Medium	Failing	1.1	= 1.2

Posture Rules

7 Failing, 2 Passing

Rule	Risk	State	Violations	Exceptions
Privileged accounts without MFA enabled	High	Passing	—	—
Slack Connect recently created external teams	High	Passing	—	—
Workspace owner accounts	High	Failing	6	—
Public channels with guests	Medium	Failing	1	—
Slack Connect externally accessible channels	Medium	Failing	17	—
Users with SMS MFA enabled	Medium	Failing	2	—
Accounts with external email domains	Low	Failing	362	—
Accounts without native MFA enabled	Low	Failing	350	—
Unaccepted invitations	Low	Failing	11	—

Security Related Posture Settings

No existing settings

Posture Rules

23 Failing, 2 Passing

Rule	Risk	State	Violations	Exceptions
Account admins	Critical	Failing	14	—
Security admins	Critical	Failing	14	—
Privileged users without MFA	High	Failing	14	—
Procedures owned by privileged system roles	High	Failing	36	—
Procedures running with privileged system roles	High	Failing	36	—
Tasks owned by privileged system roles	High	Failing	15	—
Tasks run with privileged system roles	High	Failing	11	—
Custom roles above security admin or account admin in role hierarchy	Medium	Passing	—	—
Users with no user level network policy that can bypass your identity provider	Medium	Passing	—	—
Critical databases, schemas and tables with low data retention	Medium	Failing	7	—
Critical databases, schemas and tables with no row access policies	Medium	Failing	18	—
Inactive privileged users	Medium	Failing	5	—
Non-privileged users without MFA	Medium	Failing	43	—
Schemas with no data masking	Medium	Failing	139	—
Schemas with no managed access	Medium	Failing	139	—
Service accounts with non RSA key pair login options	Medium	Failing	9	—
Users that can bypass your identity provider	Medium	Failing	55	—
Users with RSA key pair and password	Medium	Failing	2	—
Users with privileged default roles	Medium	Failing	13	—
Account admins with no email	Low	Failing	1	—
External stages with no storage integration	Low	Failing	18	—
Inactive non-privileged users	Low	Failing	7	—
Password policies with short minimum length requirement	Low	Failing	1	—
SCIM security integrations	Low	Failing	1	—
SSO security integrations	Low	Failing	1	—

Security Related Posture Settings

8 Failing, 1 Passing, 1 Other

Setting	Risk	State	Value	Target
Client session keep alive	High	Passing	false	= false
Activate policy	High	Failing		not empty
Prevent unload to inline url	High	Failing	false	= true
Prevent unload to internal stages	High	Failing	false	= true
Require storage integration for stage creation	High	Failing	false	= true
Require storage integration for stage operation	High	Failing	false	= true
Periodic data rekeying	Medium	Failing	false	= true
Tri-Secret Secure	Medium	No data	null	= true
Client encryption key size	Low	Failing	128	= 256
Minimum data retention time in days	Low	Failing	0	>= 7

Posture Rules

2 Failing, 3 Passing

Rule	Risk	State	Violations	Exceptions
Remove inactive non-privileged accounts	Medium	Passing	—	—
Remove inactive privileged accounts	Medium	Passing	—	—
Remove privileged users from low reputation domains	Medium	Passing	—	—
Remove external users with privileged access	Medium	Failing	4	—
Upgrade users with old Zoom clients	Medium	Failing	7	—

Security Related Posture Settings

25 Failing, 13 Passing

Setting	Risk	State	Value	Target
Account password - Specify a password length	High	Failing	8	>= 9
Allow use of end-to-end encryption	High	Failing	false	= true
Customize data centers for meeting/webinar/whiteboard/note...	High	Failing	null	not empty
Only authenticated meeting participants and webinar attendees...	High	Failing	false	= true
Only authenticated users can join meetings from Web client	High	Failing	false	= true
Allow participants to join before host	Medium	Passing	false	= false
Have a minimum password length	Medium	Passing	8	>= 8
Have at least 1 letter (a, b, c...)	Medium	Passing	true	= true
Have at least 1 number (1, 2, 3...)	Medium	Passing	true	= true
Have at least 1 special character (!, @, #...)	Medium	Passing	true	= true
Meeting Passcode	Medium	Passing	true	= true
Meeting passcode - Only allow numeric passcode	Medium	Passing	false	= false
Only allow numeric passcode	Medium	Passing	false	= false
Personal Meeting ID (PMI) Passcode	Medium	Passing	true	= true
Account password - Have at least 1 special character (!, @, #...)	Medium	Failing	false	= true

Setting	Risk	State	Value	Target
Account password - Specify the length of consecutive characters	Medium	Failing	0	>= 4
Account password - Use enhanced weak password detection	Medium	Failing	false	= true
Allow importing of photos from the photo library on the user's...	Medium	Failing	true	= false
Always display "Zoom Meeting" as the meeting topic	Medium	Failing	false	= true
Hide billing information from administrators	Medium	Failing	false	= true
Local recording	Medium	Failing	true	= false
Meeting passcode - Have at least 1 letter (a, b, c...)	Medium	Failing	false	= true
Meeting passcode - Have at least 1 number (1, 2, 3...)	Medium	Failing	false	= true
Meeting passcode - Have at least 1 special character (!, @, #...)	Medium	Failing	false	= true
Meeting passcode - Include both uppercase and lowercase char...	Medium	Failing	false	= true
Meeting passcode - Specify a password length	Medium	Failing	0	>= 6
Meeting passcode - Specify the length of consecutive characters	Medium	Failing	0	>= 4
Meeting passcode - Use enhanced weak passcode detection	Medium	Failing	false	= true
Only account admin can change users' name, profile picture, sig...	Medium	Failing	null	not empty
Waiting Room	Medium	Failing	false	= true
Notify host when participants join the meeting before them	Low	Passing	true	= true
Require passcode for participants joining by phone	Low	Passing	true	= true
Use personal meeting id (PMI) when scheduling a meeting	Low	Passing	false	= false
Use personal meeting id (PMI) when starting an instant meeting	Low	Passing	false	= false
Embed passcode in invite link for one-click join	Low	Failing	true	= false
Enable personal meeting ID	Low	Failing	true	= false
Identify guest participants in the meeting/webinar	Low	Failing	false	= true
Transform all meetings to private	Low	Failing	false	= true