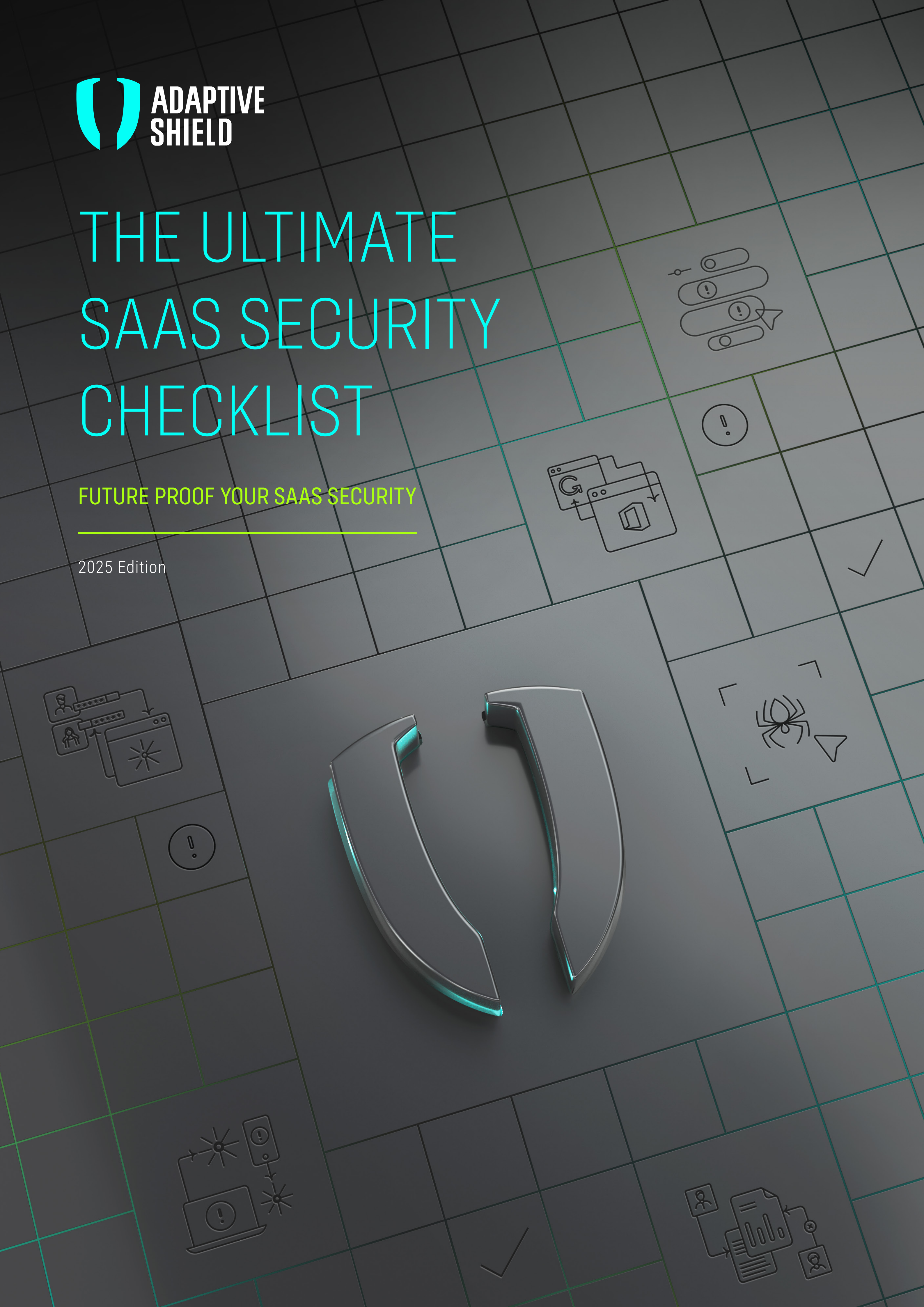
ADAPTIVE SHIELD

THE ULTIMATE SAAS SECURITY CHECKLIST

FUTURE PROOF YOUR SAAS SECURITY

2025 Edition



Contents

Intro

In the three years since we initially published the checklist, the corporate SaaS stack has grown by 32%. That means more configurations, users, devices, and data that need to be continually secured. Over the last 12 months, we've also seen GenAI introduced into SaaS applications, expanding the risk inherent in these applications. Today's SaaS attack surface has expanded exponentially, as has the number of threat actors who find it easier to access a company's cloud-based CRM than breach firewalls and on-prem servers. Meanwhile, generative AI-driven phishing attacks are leading to more compromised user accounts, more documents are shared with all, and more malicious third-party applications are being integrated into the SaaS stack.

As the challenges facing SaaS security teams mount, so does the need for a robust SaaS security platform capable of not only managing risks, but detecting threats as well. Other changes have also impacted SaaS security. The rise of SaaS has led to the democratization of SaaS security. Often, security teams lack the access and control they need to secure applications. Rather, they must rely on the application owners to secure the app.

Organizations interested in securing the SaaS stack must focus on seven areas

Misconfiguration Management

Identify configurations that introduce risk to the application.

Identity Security

Ensure only authorized users have access to the application with the least needed privileges.

Device-to-SaaS Access

Monitor the hygiene of devices accessing your apps.

3rd Party Integrated Applications

Discover integrated applications and their scopes.

Data Security

Pinpoint documents, files, repositories, and other assets that are publicly available or shared with external users.

GenAI

Mitigate risks introduced by the increased adoption of generative AI within SaaS applications.

Threat Detection

Detect real threats that could harm your apps and steal data.

This checklist will help you identify the capabilities you need from your SaaS security tool to protect your SaaS stack.

SSPM Solution

SaaS Security Posture Management (SSPM) platforms are the only way to secure all the attack surfaces hidden within your SaaS applications.

When choosing an SSPM solution, look for one with the following features and functionality.

1 **Breadth of integrations**
Includes out-of-the-box integrations.

2 **Depth of integrations**
Checks settings for every app and every user with contextual recommendation.

3 **Integration builder**
Enables users to integrate any application.

4 **Custom app security**
Integrates with and monitors custom and homegrown applications.

5 **User behavior**
Monitors and analyzes user actions to identify behavioral anomalies.

6 **Organize by organizational domain**
Provides visibility into SaaS applications by department.

7 **Posture over time**
Shows how app security posture has changed over time.

8 **Compliance**
Maps configuration settings to compliance standards.

9 **Activity monitor**
Tracks user activity and flags suspicious behaviors.

10 **Reporting**
Creates and exports SaaS security reports.

11 **RBAC**
Uses roles to control user access within the SSPM platform.

12 **Customizable security**
Enables users to modify the severity level of failed security checks to match the policy of the organization.

Misconfiguration Management

Misconfigurations can happen at any time on any application. Your SaaS Security tool should be able to automatically detect these misconfigurations, prioritize them effectively, and initiate an appropriate incident response.

When evaluating the capabilities of a SaaS security tool, look for a solution that includes these functionalities:

1 **Posture score**
Demonstrates security posture of the application and SaaS stack.

2 **Automated security checks**
24/7 checks of all configurations.

3 **Categorize by domain**
Assigns a domain for each security check, such as access control, data leakage protection, and MFA, to enable remediation prioritization.

4 **Severity level**
Assigns severity level for each security check to enable remediation prioritization and allows users to customize them.

5 **Affected users**
Displays number of users and list of users impacted by a configuration for risk assessment purposes.

6 **Compliance issues**
Associates security checks with company and industry standards to demonstrate the impact of a setting on compliance.

7 **Description of the issue**
Explains why this setting is a security concern.

8 **Remediation directions**
Provides step-by-step remediation instructions.

9 **Ticketing**
Supports ticketing systems to trigger remediation processes.

10 **Alerts**
Sends misconfiguration alerts to users.

11 **Journaling**
Allows users to document decisions relating to individual settings.

12 **SOC/SOAR/SIEM integration**
Integrates with existing security tools.

3rd Party and Shadow App Visibility

In an effort to improve productivity and extend app functionality, employees often connect their SaaS apps to third-party applications. Using OAuth authentication, these integrations are completed in seconds. However, employees rarely realize they have granted significant scopes to the third-party application.

Effective SaaS Security requires visibility into the applications that are connected to hub apps and the permissions that have been granted. For a large organization, there can be thousands of these types of apps.

Your SaaS security tool should include the following capabilities:

1 Automated app discovery
Enables security teams to see all sanctioned and unsanctioned connected apps.

2 Name of apps
Helps identify whether app is safe.

3 Users
Shows the organizational impact removing the app will have.

4 Hub app
Demonstrates which apps have apps integrated into them.

5 Scopes (how many and what they are)
Includes permissions granted to the third-party apps, such as write/delete permissions, as well as the number of scopes granted to each app.

6 Access level
Defines the permissions granted to the third-party app.

7 Connected date
Provides context to the app and the way it is used.

8 Last used date
Helps identify connected apps that are dormant.

9 Users who granted consent
Identifies users who might need training.

Identity Security Posture Management

Managing app users are of paramount importance in securing the SaaS stack. Overprivileged users, dormant users, former employees, and external users all introduce risk to the system and widen the attack surface.

Security teams need an SSPM that can monitor all human and non-human application accounts. This allows the team to understand the risk level coming from user accounts, and positions them to remove or modify access as needed.

Your SSPM tool should have the following capabilities:

1 **User discovery**
Finds all users accessing SaaS applications.

2 **User aggregation**
Combines users that login with multiple accounts into a single user.

3 **User classification**
Classifies users based on whether they are internal or external to the organization.

4 **Privileged users**
Identifies users with admin rights and other privilege permissions.

5 **Apps used**
Lists all SaaS apps and privileges for each application.

6 **Misconfigurations**
Displays all high-risk configuration settings associated with a user.

7 **User devices**
Lists all devices used to access SaaS apps.

8 **Dormant users**
Finds users who haven't accessed the application for a set time period.

9 **Deprovisioned users**
Finds former employees who retained access to the application.

10 **Overprovisioned users**
Identifies users whose permission sets exceed the needs of their role.

11 **Non-human account management**
Manages non-human accounts together with human accounts.

12 **Unusual user behavior**
Detect anomalous behaviors that could indicate an account takeover or an insider threat.

Some applications, including Salesforce and M365, have complex permission interfaces, with layers of permissions, profiles, and permissions sets, overlapped by custom permissions. Your SSPM should be able to fully monitor user permissions.

Permissions Inventory

1 **View users by profile**
See all users by profile.

2 **View permissions by user**
See all permissions granted to a single user.

3 **Manage all tenants in a unified view**
Monitor users from all instances.

4 **Discover active users to offboard**
Find users who retained access after leaving a company.

5 **Permission drill down**
Presents level of risk stemming from each user's access across all applications.

Device-to-SaaS User Risk Management

User devices pose a risk to corporate SaaS applications. Unmanaged devices and devices that are not updated are susceptible to data theft and keystroke logger malware that hands over SaaS login credentials to threat actors. Lost devices can also provide a gateway for threat actors to enter a SaaS application. When the compromised device belongs to a high-privilege user, the risk to the application increases exponentially.

Security teams require insight into the devices accessing the applications and their users. This allows them to better understand the risk coming from devices, and take necessary steps to ensure the applications are secure.

Your SSPM solution should be capable of integrating with endpoint protection platforms, unified device management platforms, or vulnerability management platforms, so it can monitor the devices that are accessing your SaaS Stack.

It should also have the following capabilities.

1 **Device information**
Lists device name, user name, platform, and operating system should all be available through the SSPM.

2 **Device status**
Shows whether device is managed and compliant with company policy.

3 **Integration with endpoint security tools**
Connects with the endpoint protection tool used by your company, such as Crowdstrike, Tenable, and SentinelOne, and alerts security users when devices have low posture.

4 **Correlate devices with users**
Recognizes which users are accessing SaaS applications using high-risk devices.

5 **Alerts in high-risk scenarios**
Identifies high-privilege users accessing SaaS applications with low-hygiene devices and triggers alerts.

6 **Lists vulnerabilities**
Shows all device vulnerabilities, ranked by priority level.

7 **Remediation guidance**
Provides step-by-step remediation guidance for vulnerabilities.

Data Management

SaaS applications contain sensitive information that could cause considerable harm to the company if they were made public. Additionally, many SaaS users share files from their SaaS applications with external users, such as contractors or agencies, as part of their operational process.

Security teams need visibility into the shared settings of documents that are publicly available or externally shared. This visibility enables them to close gaps in document security and prevent data leaks from occurring.

Your SaaS security solution should include these capabilities in the area of data leakage protection:

1 **Access level**
Displays whether item is externally or publicly shared.

2 **Owner**
Shows item's owner.

3 **Last modified**
Adds context as to whether the resource should continue to be shared.

4 **Password protected**
Shows whether publicly facing resources have a level of security.

5 **Expiration date**
Shows whether the link will expire automatically and no longer be accessible by the public.

6 **Shared with**
Includes a list of users who have been granted access to the document.

7 **File source**
Location where file is stored.

Generative AI

Generative AI is increasingly being added as a feature in SaaS applications. Add-ons such as Salesforce Einstein Copilot and Microsoft Copilot use generative AI to create reports, write proposals, and email customers. The ease of using GenAI tools has increased the risk of data leakage, expanded the attack surface, and opened new areas for exploitation.

Modern SSPMs must prioritize GenAI security to reduce the risks of a GenAI engine oversharing proprietary data or having unauthorized users gain access to these tools.

When evaluating a SaaS security solution, make sure it includes GenAI monitoring, including:

1 **Security posture for AI apps**
Score to identify AI-driven applications with heightened risk levels (e.g., Copilot apps).

2 **GenAI security checks**
Checks of all GenAI configurations, weighted by severity.

3 **GenAI remediation**
Step-by-step directions to secure GenAI configuration drifts.

4 **GenAI access**
Monitor user access to GenAI tools based on roles.

5 **GenAI shadow app discovery**
Identify shadow apps using GenAI, including malicious apps.

6 **GenAI shadow app management**
Manage shadow apps using GenAI.

7 **Manage 3rd-party AI-sanctioned apps**
Oversee interconnected GenAI apps and their level of risk, including permission scopes.

8 **Secure homegrown GenAI apps**
Integrate and monitor GenAI apps created in-house.

9 **Govern data management**
Control which data is accessible by GenAI tools.

10 **Manage GenAI device risk**
Associate users accessing GenAI SaaS applications using high-risk devices.

Identity Threat Detection and Response

Identity Threat Detection & Response (ITDR) provides a second layer of protection to the SaaS stack. This is a critical piece of the identity fabric used to secure apps, which provides security teams with another opportunity to disarm serious threats that are in motion.

When threat actors breach an application, ITDR detects and responds to identity-related threats based on detecting key Indicators of Compromise (IOCs) and User and Entity Behavior Analytics (UEBA). This triggers an alert and sets the incident response mechanism in motion. Your SSPM should include ITDR capabilities that are based on data coming from the entire SaaS stack. By extending the data collected across the SaaS stack, the ITDR tools have a far richer understanding of standard user behavior, and can better protect against threat actors.

Your SaaS Security ITDR should be able to detect the following indicators of compromise:

1 Anomalous tokens

Identify unusual tokens, such as a access token with extremely long validity period or a token that is passed from an unusual location.

2 Anomalous behavior

User acts differently than usual, such as uncharacteristically downloading high volumes of data.

3 Failed login spike

Multiple login failures using different user accounts from the same IP address.

4 Geographic behavior detection

A user logs in from two locations within a short timeframe.

5 Malicious SaaS applications

The installation of a third-party malicious SaaS application.

6 Password spray

User logs in using password spray to access a SaaS application.

ITDR should include the following capabilities

1 **Threat prioritization**
Defines the severity of the threat so the incident response team can take appropriate action.

2 **Threat description**
Describes the nature of the threat so the incident response team understands the issue.

3 **Threat target**
Identifies the app or apps that are under attack so the incident response team can secure the application.

4 **Source**
Includes the source of the alert to aid in investigation.

5 **Remediation guidance**
Provides step-by-step directions to guide the investigation and eliminate the threat.

6 **MITRE ATT&CK**
Maps attack to the MITRE ATT&CK framework.

7 **Events**
Adds context into the threat with a list of related events.

8 **SOAR and SIEM integration**
Improves threat correlation and enriches events through seamless integration with existing SOAR and SIEM tools.

9 **Communication tool integration**
Connects with your preferred communication channel to receive alerts over email, Slack, Teams, and other channel.

Final Thoughts

The Right SSPM Solution Prevents the Next Attack

At Adaptive Shield, we liken SSPM to brushing one's teeth. It's a foundational requirement that creates a state of preventive protection. We work hard to ensure Adaptive Shield is a best-of-breed SSPM solution that provides organizations continuous, automated surveillance of all SaaS apps, alongside a built-in knowledge base to ensure the highest SaaS security hygiene.

Using Adaptive Shield, security teams will deploy best practices for SaaS security, while integrating with all types of SaaS applications—including video conferencing platforms, customer support tools, HR management systems, dashboards, workspaces, content, file-sharing applications, messaging applications, marketing platforms, and more.

ADAPTIVE SHIELD

Adaptive Shield's framework is easy to use, intuitive to master, and takes five minutes to deploy.

Learn more about how you can secure your company's SaaS security now?

REQUEST A DEMO TODAY

Checklist

SSPM Solution

- □ Breadth of integrations
- □ Depth of integrations
- □ Integration builder
- □ Custom app security
- □ User behavior
- □ Organize by organizational domain
- □ Posture over time
- □ Compliance
- □ Activity monitor
- □ Reporting
- □ RBAC
- □ Customizable Security

Misconfiguration Management

- □ Posture score
- □ Automated security checks
- □ Categorize by domain
- □ Severity level
- □ Affected users
- □ Compliance issues
- □ Description of the issue
- □ Remediation directions
- □ Ticketing
- □ Alerts
- □ Journaling
- □ SOC/SOAR/SIEM Integration

Permission Inventory

- □ View users by profile
- □ View permissions by user
- □ Manage all tenants in a unified view
- □ Discover active users to offboard
- □ Permission drill down

SaaS-to-SaaS Access

- □ Automated app discovery
- □ Name of apps
- □ Users
- □ Hub app
- □ Scopes
- □ Access level
- □ Connected date
- □ Last used date
- □ Users who granted consent

Identity Security Posture Management

- □ User discovery
- □ User aggregation
- □ User classification
- □ Privileged users
- □ Apps used
- □ Misconfigurations
- □ User devices
- □ Dormant users period
- □ Deprovisioned users
- □ Overprovisioned users
- □ Non-human account management
- □ Unusual user behavior

Device-to-SaaS User Risk Management

- □ Device information
- □ Device status
- □ Integration with endpoint security tools
- □ Correlate devices with users
- □ Alerts in high-risk scenarios
- □ Lists vulnerabilities
- □ Remediation guidance

Data Management

- □ Access level
- □ Owner
- □ Last modified
- □ Password protected
- □ Expiration date
- □ Shared with
- □ File source

Generative AI

- □ Security posture for AI
- □ GenAI security checks
- □ GenAI remediation
- □ GenAI access
- □ GenAI shadow app discovery
- □ GenAI shadow app management
- □ Manage 3rd-party AI-sanctioned apps
- □ Secure homegrown GenAI apps
- □ Govern data management
- □ Manage GenAI device risk

Identity Threat Detection and Response

Threats it should detect:

- □ Anomalous tokens
- □ Anomalous behavior
- □ Failed login spike
- □ Geographic behavior detection
- □ Malicious SaaS applications
- □ Password spray attacks

ITDR should include the following capabilities:

- □ Threat prioritization
- □ Threat description
- □ Threat target
- □ Source
- □ Remediation guidance
- □ MITRE ATT&CK
- □ Events
- □ SOAR and SIEM integration
- □ Communication tool integration