











Wing Security Basic

What is Wing Security basic and what is included with it?

Suited for organizations starting to protect their SaaS domain and are looking to automate shadow IT risk management, user access, and manage SaaS compliance. Wing's Basic tier automatically manages your SaaS app risks, application onboarding process, and User Access management.

-  **Apps:** Discover your organization's entire SaaS supply chain, spanning your workspace, major platforms, and employee email accounts. Utilize Wing's 300,000-app reputation database to automate risk management, addressing both risky applications and their AI learning risks. Wing provides customers visibility to assess knowledge leakage risks within AI-based SaaS supply chains, displaying AI features in applications along with their relevant terms and conditions regarding data training and learning.
-  **Users:** Discover all users and applications and conduct User Access Reviews for dozens of apps from one platform. Select manual actions to manage your employee access.
-  **Data:** Wing's Basic tier provides visibility into SaaS data sharing.
-  **Threat intelligence, Detection and Response:** Wing's Basic tier offers insights into security events occurring within your SaaS supply chain.
-  **Efficiency and Support:** Customers benefit from access to online support and new feature guides.

What is not included in the Basic Tier?

-  **Apps:** Discovery of apps used on employee devices (not discoverable in workspace or mail accounts). Automatic reduction of attack surface through the detection of changes in the app's security posture and managing unused or over-provisioned apps. MFA usage tracking and misconfiguration for SaaS platforms also not included. Automatic alerts and automatic workflow related to changes in AI risks posture.
-  **Users:** Continuous monitoring of app users to automatically control access and off-boarding and prevent over-provisioning of users and admins.
-  **Data:** Automated or manual actions to reduce misconfiguration and data exposed with risky sharing methods or sensitive file sharing.
-  **Event Detection and Response:** Automatic alerts and playbooks for security incidents in your SaaS supply chain and compromised employee credentials. Scan for risky user behaviors or abnormal data movement between apps and users.
-  **Efficiency and Support:** Comprehensive integration to SOAR/SEIM system, support SSO, and ticketing systems.

Wing Security Basic

	Discovery	Posture Management	Detection and Response
Apps	<p>Automatic:</p> <ul style="list-style-type: none"> • Comprehensive SaaS discovery <ul style="list-style-type: none"> ◊ From workspace & IAM ◊ App2App (API) ◊ Mail server • 300,000 SaaS app reputation database • AI Risks + T&C tracking of AI use 	<p>Automatic management:</p> <ul style="list-style-type: none"> • App onboarding flows • App risk management 	<p>Manually View:</p> <ul style="list-style-type: none"> • Threat intelligence for used apps
Users	<p>Automatic:</p> <ul style="list-style-type: none"> • Access to applications • Role detection • User Access Reviews 	<p>Manual:</p> <ul style="list-style-type: none"> • Select off-boarding actions 	
Data	<p>Automatic:</p> <ul style="list-style-type: none"> • Exposed assets visibility 		
Additional Services	<ul style="list-style-type: none"> • Online support • Online features and usage guide 		