Wing Security Enterprise

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

Suited for organizations requiring the most comprehensive automated risk reduction across SaaS apps utilized by business units and employees. An Enterprise solution that automatically reduces your SaaS risks across **apps**, their **users**, and the **data** that is being shared.

Apps: Discover your organization's entire SaaS supply chain, including all apps linked to your workspace, major SaaS platforms, employee email accounts, and monitored devices. Utilize Wing's database of 300,000 SaaS apps to automate risk management, identifying risky applications and their AI learning capabilities. Wing Enterprise detects and remediates knowledge leakage risks in AI-based SaaS supply chains by scanning for new AI features, monitoring T&C changes, and automating onboarding and security remediation. The Enterprise tier actively reduces attack surface by detecting changes in app security posture and managing unused or over-provisioned apps. Benefit from comprehensive app usage and misconfiguration monitoring, along with professional reviews of key SaaS platforms.

Users: Continuously monitor users of applications for automated access control, enforcement of MFA configurations, proper off-boarding, and prevention of user and admin over-provisioning.

Data: Oversee data sharing across apps and automatically reduce misconfigurations, mitigating data leakage risks associated with risky sharing methods or sensitive file sharing.

Threat intelligence, Detection and Response: Wing's Enterprise tier offers Wing's most comprehensive tools for timely security incident alerts, tracking compromised employee credentials, and monitoring risky user behaviors and abnormal data movement across apps and users in your SaaS supply chain.

Efficiency and Support: Customers enjoy specialized support, frequent feature updates, and the most comprehensive integration with SOAR/SEIM systems, SSO, and ticketing systems.

Wing Security Enterprise

	Discovery	Posture Management	Detection and Response

Apps	**Automatic:**
	• Full SaaS discovery
	  ◇ From workspace & IAM
	  ◇ App2App (API)
	  ◇ Mail server
	  ◇ Managed devices
	• 300,000 SaaS app reputation database
	• AI Risks + T&C tracking of AI use
		Automatic management of:
		• App onboarding flows
		• App risk & posture changes
		• AI T&Cs and training risk changes
		• Misconfigurations
		• Unused apps
		• Overprovisioned apps
			Automatic management of:
			• App threat intelligence
			• App security events
			• Response playbooks

Users	**Automatic:** • Access to applications • Internal/External users • Role detection • User Access Reviews	**Automatic:** • Offboarding • MFA configuration & enforcement • Over permission reduction • Admin under-usage • Unused external access removal	**Automatic:** • Credential leak detection • Risky behavior detection
Data	**Automatic:** • Exposed assets and owners	**Automatic:** • Reduction of risky shares • Reduction of unused share • Apps sharing misuse	**Automatic alert on:** • Abnormal data movement • Data forwarding
Additional Services	• SOAR/SIEM/Ticketing system integration • SSO • Dedicated support engineer		