ADAPTIVE SHIELD

Adaptive Shield Solution Overview

USE CASES & CORE CAPABILITIES

Secure Your Entire SaaS Stack

Gain deep, continuous visibility and control over your SaaS stack. Adaptive Shield's SaaS Security Platform empowers you to prevent, detect, and respond to SaaS threats. Easily collaborate with your app owners to fix any security drift.

Stay on Top of Security Misconfigurations

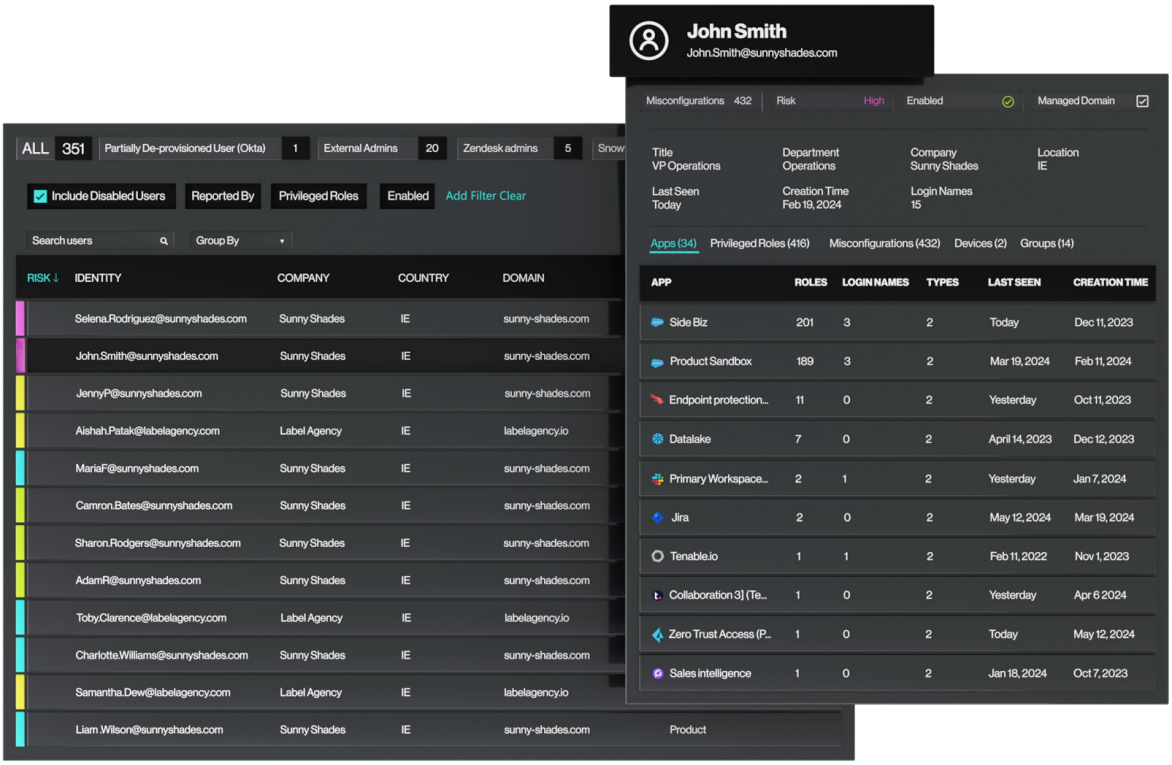
Integrate with all SaaS apps to monitor and manage security misconfigurations through in-depth security checks and auto/step-by-step remediation.

With Adaptive Shield you can achieve:

- App breadth & security depth
- Risk management prioritization by severity or security domain
- Guided remediation
- Compliance mapping

Build a Strong Identity Security Posture

Strengthen governance of internal and external SaaS users, monitor permissions, and secure non-human identities.



Privileged Roles

Identify privileged users to prioritize misconfiguration management, device management, and third party app access.

Permission Trimming

Implement the Principle of Least Privilege (PoLP) and ensure each SaaS user has the right level of access needed while still enabling business operations.

User Deprovisioning

Detect users who have been disabled in the Active Directory but retained access to SaaS apps, dormant users, and privileged accounts from external domains.

User Classification

Identify which users are external, internal, non-human, and any other categorization of choice.

Discover Connected & Shadow Apps

Detect and control all sanctioned and unsanctioned SaaS apps and other integrations connected to your core SaaS stack that can pose a risk to your business.

App Discovery

Discover and Control 3rd party app access, connected to your core SaaS stack.

Malicious App Discovery

Identify malicious applications and gather forensics through the activity monitoring panel. These applications put data at risk of ransomware, theft, and destruction.

Measure Risk Level of Connected Apps

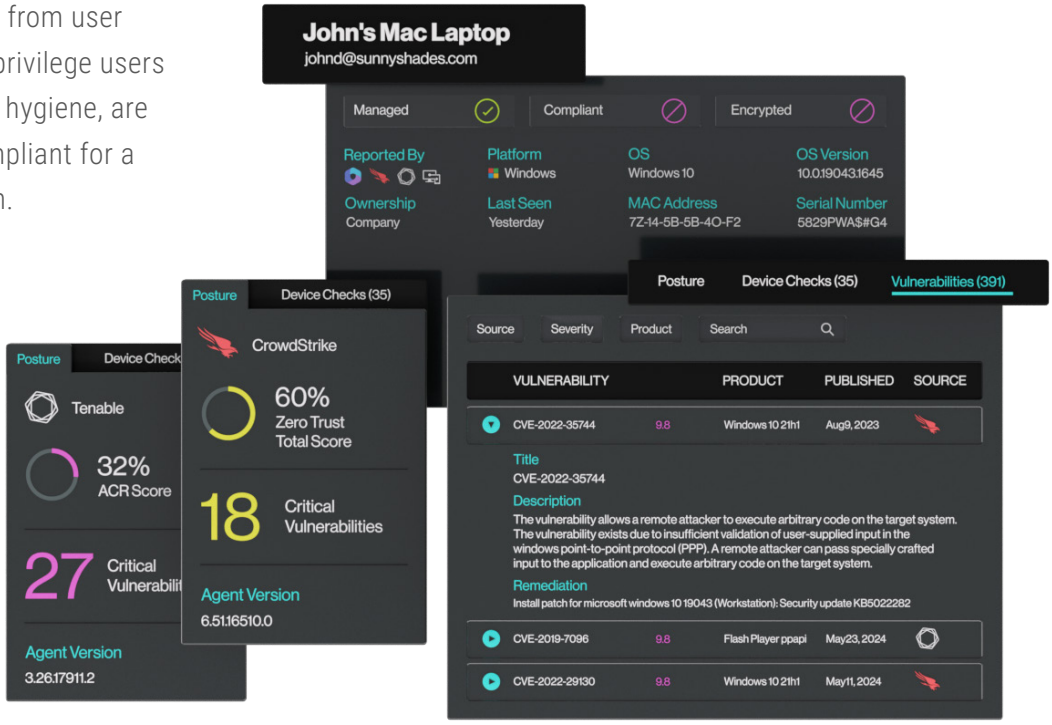
Once connected applications are detected, understand which ones request high-risk scopes.

Dormant App Discovery

Find high-risk applications that have access to the SaaS stack but haven't been accessed over long periods of time.

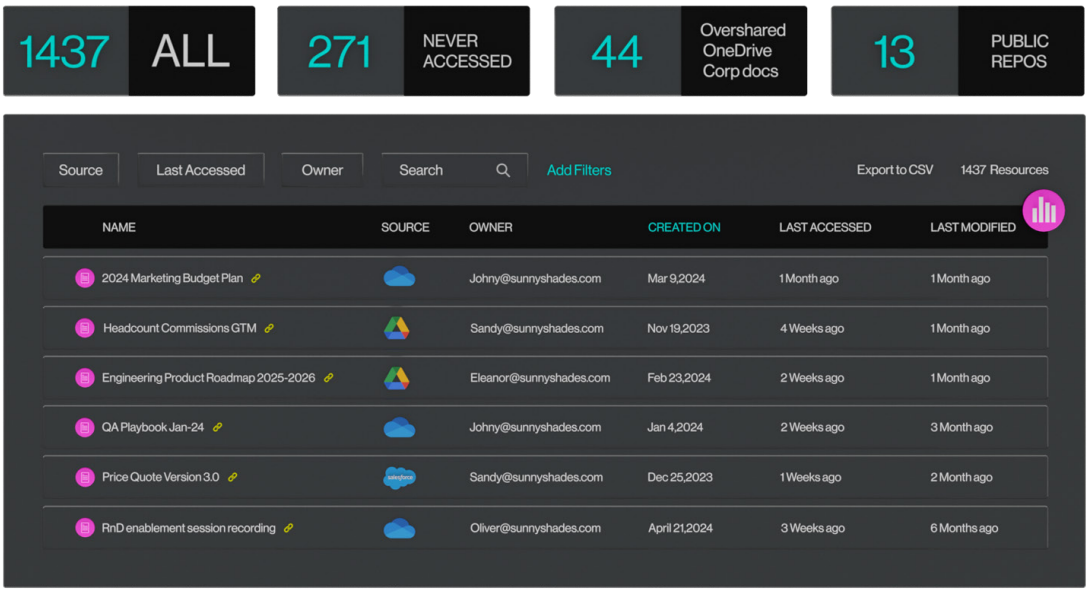
Manage Device Risk

Manage SaaS risks deriving from user devices and prioritize high-privilege users with devices that have poor hygiene, are unmanaged, or are non-compliant for a holistic Zero Trust approach.



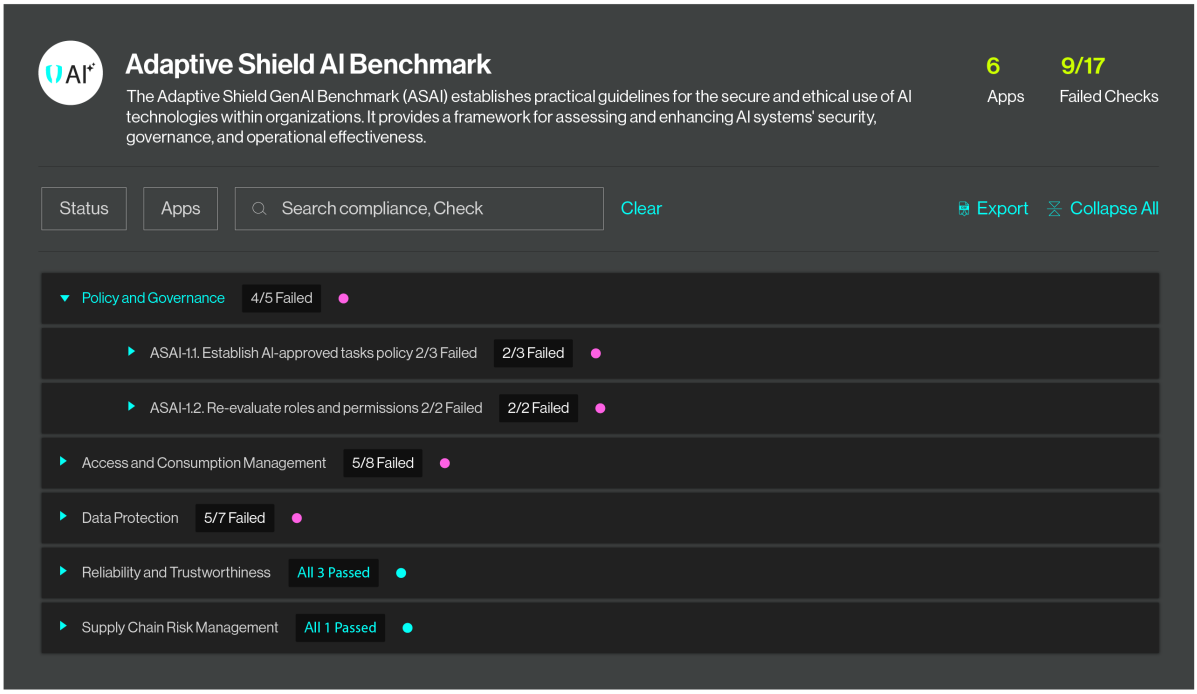
Gain Visibility into Data Exposure

Discover public and externally shared documents, files, code repositories, and calendars to prevent data leaks and limit phishing attacks.



Get a Handle on GenAI

Take control of GenAI tools in your SaaS stack to prevent data leakage and unauthorized access.



Security Posture for AI Apps

Delve into the security posture of any AI application and address configuration drifts.

AI Configurations

Control AI-related security settings within SaaS applications to prevent data leakage or any exposure.

AI Shadow Apps

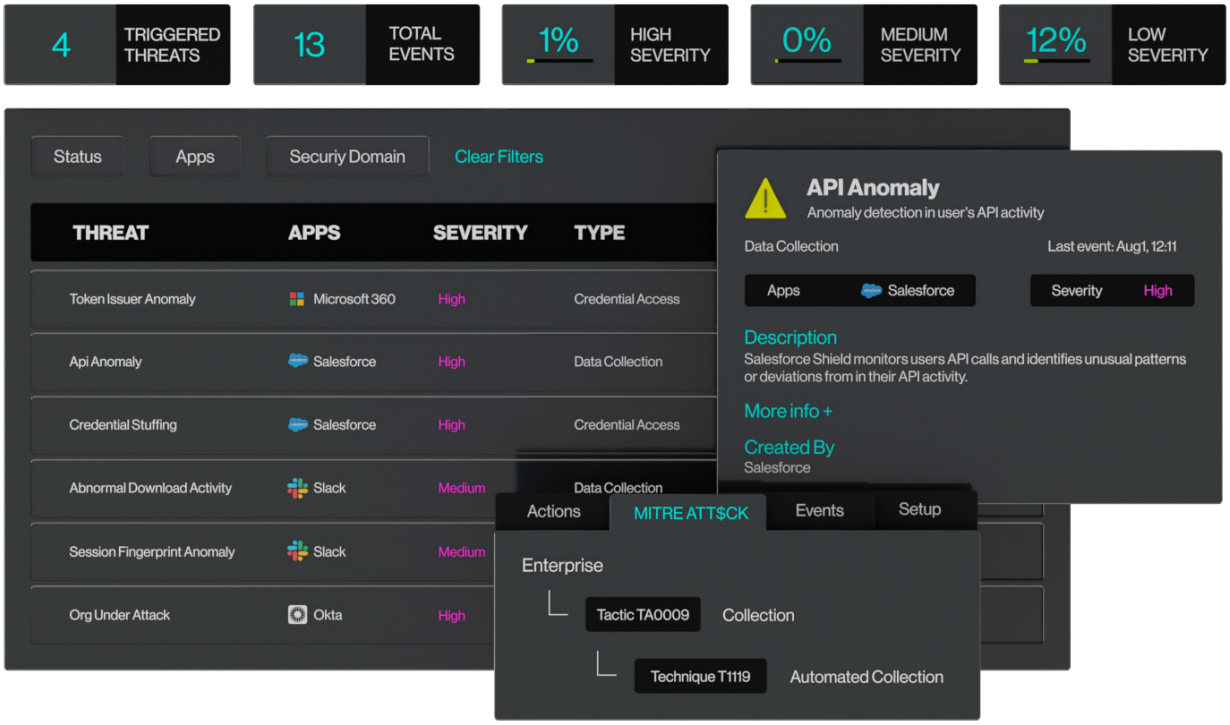
Identify GenAI Shadow apps, including suspected malicious applications, to automatically revoke access based on their risk level.

AI 3rd Party Sanctioned Apps

Oversee interconnected GenAI applications and the level of risk they pose to the SaaS hubs, including reviewing permission scopes.

Detect and Respond to Threats

Adaptive Shield collects evidence indicating that the organization's SaaS apps are under attack or have been compromised by identifying common Tactics, Techniques and Procedures (TTPs) used by adversaries. This is done by detecting Indicators of Compromise (IOC) and User & Entity Behavior Analytics (UEBA).



MITRE ATT&CK Mapping

Improve threat detection and incident response based on the MITRE ATT&CK framework.

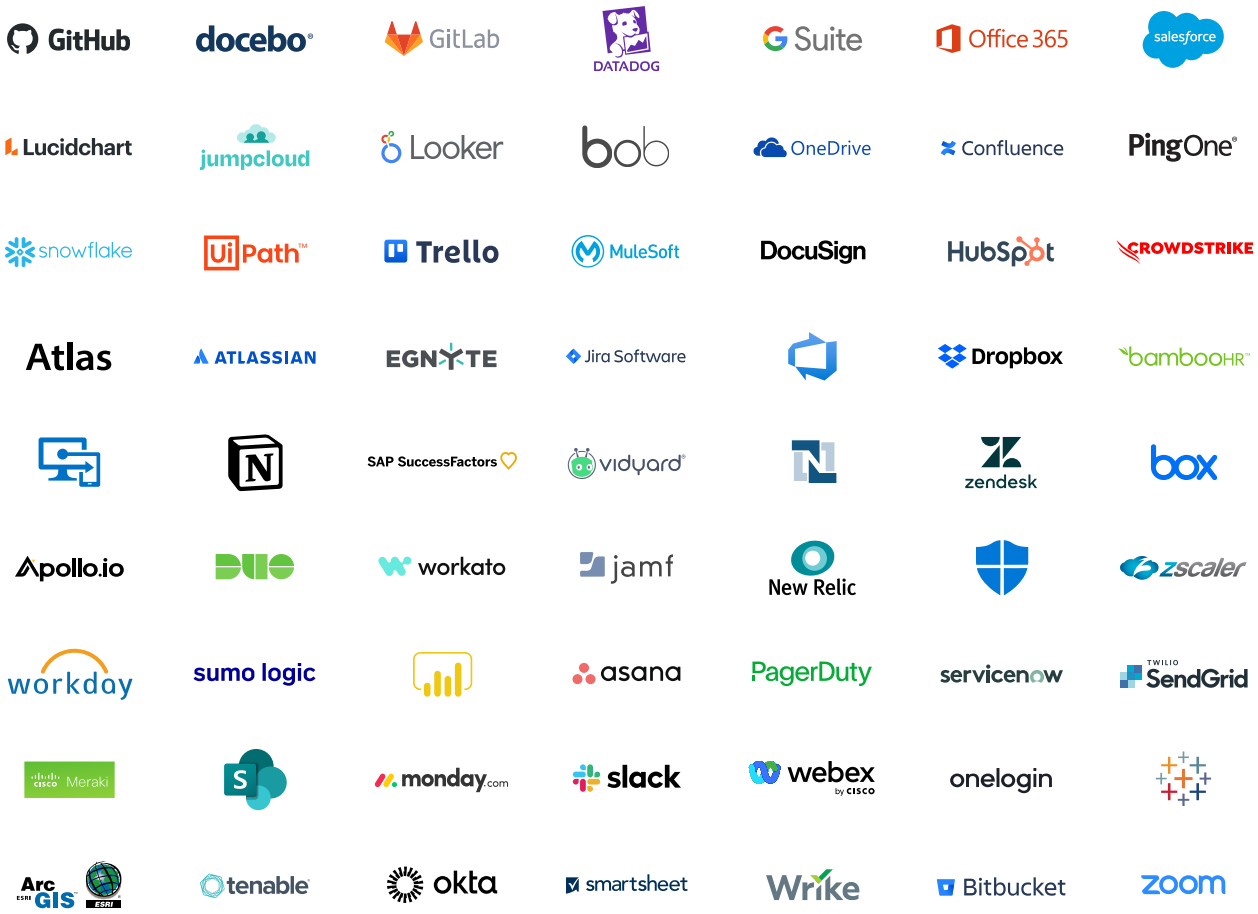
Alerts and SIEM & SOAR Integrations

Receive timely notifications in multiple channels such as email, Slack, or Teams, indicating potential threats that requires immediate investigation or response. Seamlessly integrate with your existing Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools.

Remediation Guidance

Get actionable insights and step-by-step guidance to address and mitigate vulnerabilities, weaknesses, or compromises in the event of a security incident.

Adaptive Shield is the only SSPM with out-of-the-box support for over 160 SaaS applications



About Adaptive Shield

Adaptive Shield, leader in SaaS Security, enables security teams to secure their entire SaaS stack through threat prevention, detection, and response. With Adaptive Shield, organizations continuously manage and control all SaaS and 3rd-party connected apps, as well as govern all SaaS users and risks associated with their devices. Founded by Maor Bin and Jony Shlomoff, Adaptive Shield works with many Fortune 500 enterprises and was named Gartner® Cool Vendor™ 2022.

For more information, visit us at adaptive-shield.com or follow us on LinkedIn.