

# Adaptive Shield Solution Overview

0.

5

5

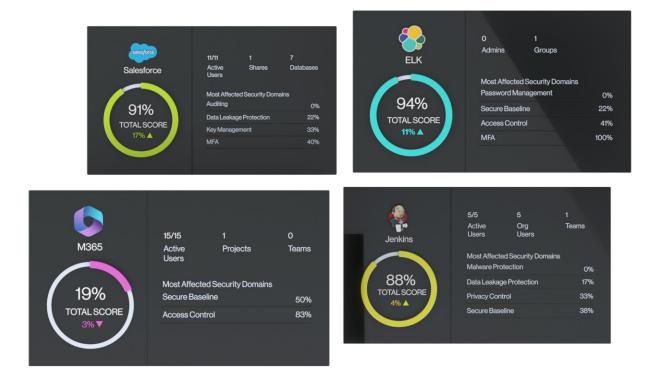
**USE CASES & CORE CAPABILITIES** 

## 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.

	John Smith John Smith@surnyshades.com										
					Misconfigurations 432	Risk		Enabled	🧭 Mana	ged Domain 🔽	
	Partially De-provisioned User (Okta)           lude Disabled Users         Reported By	1 External Adm	ins 20 Zende Enabled Add Filte	skadmins 5 Snow r Clear	Title VP Operations Last Seen Today	Departmer Operations Creation Ti Feb 19, 202	ne	Company Sunny Shades Login Names 15	Loca IE	tion	
Search	Searchusers Q Group By +					Apps (34) Privileged Roles (416) Misconfigurations (432) Devices (2) Groups (14)					
<b>RISK</b> ↓	IDENTITY	COMPANY	COUNTRY	DOMAIN	АРР	ROLES	LOGIN NAMES	TYPES	LAST SEEN	CREATION TIME	
	Selena.Rodriguez@sunnyshades.com	Sunny Shades	IE	sunny-shades.com	👄 Side Biz	201			Today	Dec 11, 2023	
	John.Smith@sunnyshades.com	Sunny Shades	IE	sunny-shades.com	Product Sandbox	189			Mar 19, 2024	Feb 11, 2024	
	JennyP@sunnyshades.com	Sunny Shades	IE	sunny-shades.com	Sendpoint protection				Yesterday	Oct 11, 2023	
	Aishah.Patak@labelagency.com	Label Agency	IE	labelagency.io	A Datalake				April 14, 2023	Dec 12, 2023	
	MariaF@sunnyshades.com	Sunny Shades	IE	sunny-shades.com	Primary Workspace				Yesterday	Jan 7, 2024	
	Camron.Bates@sunnyshades.com	Sunny Shades	IE	sunny-shades.com	ᅌ Jira				May 12, 2024	Mar 19, 2024	
	Sharon.Rodgers@sunnyshades.com	Sunny Shades	IE	sunny-shades.com	O Tenable.io			2	Feb 11, 2022	Nov 1. 2023	
	AdamR@sunnyshades.com	Sunny Shades	IE	sunny-shades.com	t. Collaboration 3] (Te		0	2	Yesterday	Apr 6 2024	
	Toby.Clarence@labelagency.com	Label Agency	IE	labelagency.io				2			
	Charlotte.Williams@sunnyshades.com	Sunny Shades	IE	sunny-shades.com	Zero Trust Access (P				Today	May 12, 2024	
	Samantha.Dew@labelagency.com	Label Agency	IE	labelagency.io	Sales intelligence		0	2	Jan 18, 2024	Oct 7, 2023	
	Liam .Wilson@sunnyshades.com	Sunny Shades	IE	sunny-shades.com	Product						

## 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.



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.

#### **John's Mac Laptop** johnd@sunnyshades.com Managed Encrypted OS Windows 10 OS Version 10.0.19043.1645 0 **>** 🔿 🛱 Windows MAC Address 7Z-14-5B-5B-4O-F2 Serial Number Com vice Checks (35) Post abilities (391) Device Checks (35) Product CrowdStrike Device Chec VULNERABILITY PRODUCT PUBLISHED SOURCE 60% Tenable $\bigcirc$ Zero Trust Total Score CVE-2022-35744 32% Title CVE-2022-35744 ACR Score Critical Vulnerabilities Critical Vulnerabili Agent Version 6.51.16510.0 0 0 CVE-2019-7096 Agent Version 3.26.17911.2 CVE-2022-29130 Mav11.202

## Gain Visibility into Data Exposure

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

1437 ALL	271	NEV	er ESSED 44	Oversha OneDriv Corp doo	13	PUBLIC REPOS
Source Last Accessed	Owner	Search	Q Add Filters		Export to C	SV 1437 Resources
NAME		SOURCE	OWNER	CREATED ON	LAST ACCESSED	
2024 Marketing Budget Plan 🥜			Johny@sunnyshades.com	Mar 9,2024	1 Month ago	1 Month ago
Headcount Commissions GTM 8			Sandy@sunnyshades.com	Nov 19,2023	4 Weeks ago	1 Month ago
Engineering Product Roadmap 202	25-2026 🔗		Eleanor@sunnyshades.com	Feb 23,2024	2 Weeks ago	1 Month ago
QA Playbook Jan-24 🤌			Johny@sunnyshades.com	Jan 4,2024	2 Weeks ago	3 Month ago
Price Quote Version 3.0 🤌			Sandy@sunnyshades.com	Dec 25,2023	1 Weeks ago	2 Month ago
RnD enablement session recording	g 🖉		Oliver@sunnyshades.com	April 21,2024	3 Weeks ago	6 Months ago



## Get a Handle on GenAI

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

Adaptive Shield Al Benchmark The Adaptive Shield GenAl Benchmark (ASAI) establishes practical guidelines for the secure and ethical use of Al technologies within organizations. It provides a framework for assessing and enhancing Al systems' security, governance, and operational effectiveness.	<mark>6</mark> Apps	<b>9/17</b> Failed Checks
Status     Apps     Q     Search compliance, Check     Clear	₿ Export	∑ Collapse All
Policy and Governance 4/5 Failed		
<ul> <li>ASAI-1.1. Establish AI-approved tasks policy 2/3 Failed</li> <li>ASAI-1.2. Re-evaluate roles and permissions 2/2 Failed</li> <li>2/2 Failed</li> </ul>		
Access and Consumption Management 5/8 Failed		
Data Protection 5/7 Failed		
Reliability and Trustworthiness All 3 Passed		
Supply Chain Risk Management All 1 Passed		

## Security Posture for AI Apps

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

## AI Configurations

Control Al-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.



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).

4 TRIGGERED THREATS		TAL ENTS	1% HIGH		.0%	MEDIUM SEVERITY	<u>12%</u>	LOW SEVERITY	
Status Apps	Securiy Domain	Clear F	Filters						
THREAT	APPS	SEVERI	ТҮ ТҮРЕ	D		nomaly detection in user's A	er's API activity Last event: Aug1, 12:11		
Token Issuer Anomaly	Hicrosoft 360		Credential Acces	is 🛛	Apps	Salesforce	Severity	High	
Api Anomaly	🐡 Salesforce		Data Collection	Si	escription alesforce Shield m r deviations from ir		Ils and identifies unus	sual patterns	
Credential Stuffing	🐡 Salesforce		Credential Acces	s	1ore info + Created By				
Abnormal Download Activity	👬 Slack	Medium	Data Collection Actions MITR		alesforce Events	Setup			
Session Fingerprint Anomaly	📫 Slack	Medium	Enterprise						
Org Under Attack	💭 Okta		Tactic TA00	09 Colle	ection				
			Tec	hnique T1119	Automated	d Collection			

## MITRE ATT&CK Mapping

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

## Alerts and SIEM & SOAR Integrations

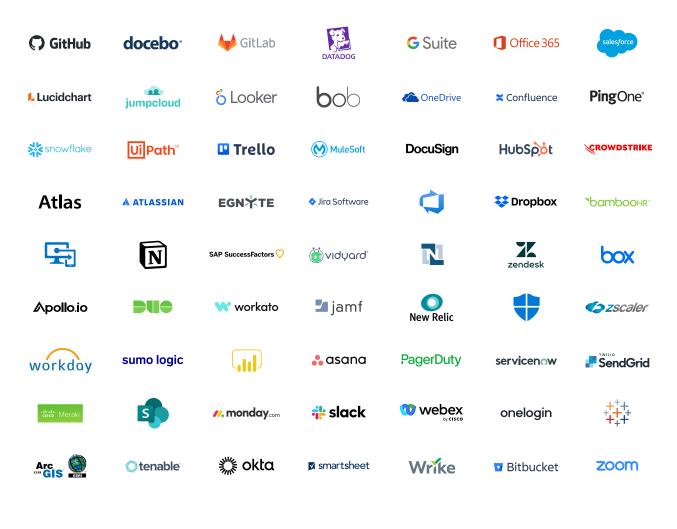
Receive timely notifications in multiple channels such as email, Slack, or Teams, indicating potential threats that requires immediate investigation or response. Seamlessly integrate with your existing Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (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<sup>®</sup> Cool Vendor<sup>™</sup> 2022.

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



