ADAPTIVE SHIELD

Identity Security Posture

Govern all users, from employees and external users to service accounts. Oversee their level of activity and permissions across the entire SaaS stack.

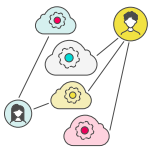
Every user identity is a potential entrance into the SaaS application. Adaptive Shield focuses on strengthening organizations' rich identity fabric, preventing unauthorized users from accessing corporate SaaS applications. With Adaptive Shield, you can oversee all identity-based access to apps, provide security teams with full visibility into their users, and ensure sufficient protections are in place to keep threat actors out.

60% of security experts are concerned about insufficient identity, credentials, access and key management.

Features

User Risk Level
Based on role, privilege level, and current configurations

User Inventory
See the list of active, deactivated, dormant and unmanaged users



User SaaS Profile
View user roles, privileges, all apps they have access to, failed security checks, devices, groups, departments, titles, last login, and all user names

Capabilities

- **Permission Trimming**
  Review access and permissions to ensure users have an appropriate level of access based on their roles and needs
- **User Deprovisioning**
  Create lists of users who are dormant, disabled in the Active Directory or LDAP, or no longer require access, deprovision their access
- **External Users**
  Track external users to ensure they still require access and manage their privileges
- **Unmanaged Users**
  Capture users with access who are not being managed by the company's IDP
- **Misconfiguration Prioritization**
  Identify users with the highest privileges and most high-risk misconfigurations to set remediation priorities

ADAPTIVE SHIELD

Identity Security Use Cases

Discover Dormant Accounts

Dormant accounts, such as those involved in the initial application setup or ones that are no longer in use, expand the attack surface by providing an additional pathway for threat actors to enter the app. These accounts often have easy-to-remember passwords and may have expansive permission sets.

Using Adaptive Shield, organizations have the visibility needed to disable or delete these dormant accounts.

Aggregate Users

Identity security requires developing a user profile based on all their online behaviors. When a user logs into different applications using different email addresses or user names, Adaptive Shield aggregates all those accounts into a single user view.

This provides organizations with a holistic view of each user's digital footprint and communication patterns.

Provisioning and Deprovisioning Users

When adding users to an application, companies should follow the principle of least privilege, and grant only the permissions needed to complete their job functions. Adaptive Shield allows organizations to compare privileges between users with similar roles, titles, and departments to ensure that the user is not over-permissioned.

When employees leave the organization, their access must be fully removed from every application. While applications that are connected to the corporate Identity Provider (IdP) will automatically remove access through SSO, users with local access must be manually deprovisioned. Adaptive Shield helps organizations discover users from across the SaaS stack that must be immediately deprovisioned.

35% of security professionals say that too many departments have access to security settings.

GitHub, docebo, GitLab, Datadog, G Suite, salesforce, Lucidchart, jumpcloud, Looker, bob, OneDrive, Confluence, PingOne, snowflake, UiPath, Trello, MuleSoft, DocuSign, HubSpot, CROWDSTRIKE, ATLASSIAN, EGNYTE, Jira Software, Dropbox, bamboohr, SAP SuccessFactors, vidyard, zendesk, box, Apollo.io, workato, jamf, New Relic, zscaler, workday, sumo logic, asana, PagerDuty, servicenow, SendGrid, Meraki, monday.com, slack, webex by cisco, onelogin, ArcGIS, tenable, okta, smartsheet, Wrike, Bitbucket, zoom

View all 140+ Supported Integrations

ADAPTIVE SHIELD

Adaptive Shield enables security teams to start securing their entire SaaS ecosystem's security by strengthening the organization's SaaS posture, and detecting and responding to SaaS threats. Founded by Maor Bin and Jony Shlomoff, Adaptive Shield works with many Fortune 500 enterprises and has been named Gartner® Cool Vendor™ 2022.

With Adaptive Shield, you can secure your SaaS stack with:

- Misconfiguration Management
- SaaS-to-SaaS Access Discovery and Control
- Identity Security Posture
- Device-to-SaaS Risk Management
- Identity Threat Detection and Response (ITDR)

www.adaptive-shield.com Follow us on LinkedIn REQUEST A DEMO