Your Data and Adaptive Shield

Adaptive Shield is fully committed to securing customer data stored within SaaS applications. As a security vendor, we often have access to the data we are tasked with securing. This document clarifies the type of access Adaptive Shield requests, the way we access data, and the measures we put in place to protect customer data.

Permissions Requested

Adaptive Shield requires specific permissions from SaaS applications to effectively monitor and analyze security-related information. These requests for access are tailored to collect only the data needed to secure applications.

Some SaaS applications have limited permission structures. In those circumstances, Adaptive Shield requests elevated administrative permissions. These permissions are only requested when no alternative is available.

Requested Data

Adaptive Shield requires the following types of data from our customers' SaaS tenants to effectively monitor applications and detect threats:

- Configuration settings – includes data related to the state of configuration settings that are involved in securing an application
- Basic user information – includes users' names, email addresses, roles, and other data that appears in the customer's user directory
- All activity logs – includes data found in sign-in logs and audit logs, such as IP addresses, user agents, and external user email addresses, as well as data that can be extrapolated from logs
- Device information – includes the device name, device owner, platform, OS, and other device-related data
- Connected applications – includes 3rd party applications, OAuth scopes, and users who were granted access to the application

Limiting this access will reduce the effectiveness of Adaptive Shield's monitoring and threat detection capabilities.

© 2024 Adaptive Shield. All Rights Reserved

Access Methods

Adaptive Shield accesses customer applications through the following methods:

OAuth Authorization

Adaptive Shield's preferred connectivity is through the SaaS application's public API. OAuth allows us to request limited scopes to perform essential monitoring tasks while reducing exposure of any sensitive data.

Service Account Credentials

When OAuth is not available or does not expose enough relevant information, we require a service account with the necessary permissions.

Other Methods

When required, Adaptive Shield uses other types of authentication based on the application vendor, including key pairing and API tokens or keys.

Security Measures to Secure Customer Data

Adaptive Shield implements the following to protect customer data:

- Encryption of credentials – any credentials and OAuth secrets given to Adaptive Shield are encrypted using a unique key assigned to each customer. The encryption is on the cell level and is in addition to at-rest encryption
- IP allowlist configuration – Adaptive Shield accesses customer SaaS applications from servers using static IP addresses. This allows customers to limit access our access to specific IP addresses using an IP allowlist
- Audit logging – every action Adaptive Shield takes is logged, creating an audit trail to track all activities and identify any anomalous behavior. These logs can be monitored by customers at any time via the Adaptive Shield platform UI, Adaptive Shield platform API, or integration with SIEM tools

Learn more at

www.adaptive-shield.com/trust-center

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 apps, including 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 has been named Gartner® Cool Vendor™ 2022.

www.adaptive-shield.com

Follow us on LinkedIn