November, 2022

Gradient MSP Privacy

gradient msp

Table of Contents

Introduction

Gradient MSP recognizes the importance of data privacy and the sensitivity of the information accessed by our platform. As many of Gradient's employees have experience in the IT channel, both as MSPs and as vendors, we understand the concerns and questions that come up when sharing data that might identify customers, business practices, market coverage, etc.

In this whitepaper, we outline some of the controls in place to protect the privacy of organizations that share data with Gradient.

Minimum Data Collection

When obtaining data from PSAs via an import, we only acquire information that is required to provide our services.

Minimum Integration Data Requirements

When vendor partners integrate with Gradient, we similarly only require data that is required for the integration to work. Our API endpoints for integrations are publicly available to review the data that is received through an integration.

As our API only allows receipt of required fields, any extraneous information is dropped.

Data Storage

All associated data is stored in Amazon Web Services in United States regions.

Data is stored encrypted at rest and is only accessed via communications mechanisms that employ encryption in transit.

Least Privilege PSA Access

When providing Gradient access to a PSA to collect data, we request that the API user or key be created with the minimum permissions required, to the degree allowed by each API.

Integration partners can only review only the data that is received via the same integration key that was used to create or send the data.

Least Privilege Access Production Access

Only limited staff have direct access to production data, and only a subset of those have write access to it. Access is granted only as needed for troubleshooting purposes.

Full Data Removal

Upon request, Gradient will completely remove all data collected about an organization from its application. Note that data may still exist in backups and/or snapshots and that this data cannot be deleted.

Inference Protection

We realize the risk of inferring identities or key business data when publishing reports or statistics. To address that risk, some of the rules we use for ourselves in reporting:

- Any statistics published about vendor partners will relate to product categories and/or subcategories only. For example, EDR or Email Security.

- Data will not be released about a category unless we integrate with at least three providers in that category to prevent inferring identity.

- For any geographic information such as state, region, etc., data won't be released unless we have at least twenty partners in that geography. This applies to both integration partners and platform users.

The same types of anti-inference controls apply to any vertical or demographic information, such as company size or revenue.

Additional Program Opt-In

Any additional programs Gradient develops or offers, outside of trend or statistic reporting will be opt-in. Specifically, these will require a discrete opt-in as opposed to an automatic opt-in.

Data Security

As part of meeting privacy obligations, Gradient also protects the security of data shared with us. Please see our Security Whitepaper for more information on the controls in place around data security.


gradient
msp