Gradient MSP Security Overview

By Matt Topper
Director of Security at Gradient MSP

gradient msp

Table of Contents

Introduction

Gradient MSP recognizes the importance of security, both of its own assets and of the access granted to us by our customers. Security is at the core of how our business operates – from our product development and training practices to our everyday operations and overall culture.

As innovators in the MSP space, we know that security is critical to developing products that our customers feel safe using. At Gradient, we recognize what access to customer data means and take our responsibility to protect it seriously. That's why customer data is protected using rigorous and closely monitored internal practices.

In this document, we outline some of the security controls in place to protect those assets. This is not a comprehensive list of all security controls nor is it a statement of compliance. Instead, we hope to present an overview of how we approach security and risk management.

Security Strategies

Some of the overarching security principles that we operate under are described below.

Least Privilege

Gradient MSP provides employees the minimum privileges required to perform their duties in all applications and infrastructure. This includes both access to assets and access within assets, such as preferring read-only access.

The least-privilege principle also applies to the access we request to outside assets, such as PSA integrations. While we need access to these resources, we only want as much access as is absolutely required for our applications to function.

Assume Control Failure

This encompasses the principles of “defense in depth” and “assume compromise”. In other words, we don’t assume that any single control or security layer is going to stop all threats, even all threats that any control is specifically designed to prevent. Instead, we prefer to have multiple, overlapping controls.

Continuous Improvement

Gradient MSP is committed to continually improving its security posture. This applies internally, to our applications, and to our development practices. We review our configuration standards, new features in tools, changing environmental factors and emerging threats to increase our security.

CIS Risk Assessment Model

For information security risk assessments, Gradient uses the CIS Risk Assessment Model. CIS RAM helps us define our acceptable level of risk and identify when to prioritize and implement the CIS Controls to manage risk. CIS RAM provides a method for evaluating risk by calculating the likelihood of an impact to customers, business objectives, and external entities.

Security Controls

Hardware Assets

Access to resources at Gradient MSP requires a corporate device, both by policy and technology. This allows us to understand what we have deployed and ensure that it’s in the proper state before it connects to our information assets.

For application hosting, infrastructure is deployed as code, providing a built-in inventory of current systems.

In cases where a policy exception was made, such as a service that does not integrate with our identity management system, compensating controls exist to limit the exposure from unauthorized access to such systems.

Software Assets

Gradient MSP requires that new third-party software services be approved prior to use. This process evaluates an application's security controls and potential exposure for compromise before use.

Encryption

Data within Gradient MSP's application database is encrypted using industry-standard algorithms and key lengths. All data in transit is encrypted with TLS.

All Gradient MSP endpoints and mobile devices are encrypted. This status is confirmed before access is granted to resources.

People

Gradient MSP employees and contractors undergo a thorough background check before starting employment.

Prior to being granted access to any organizational data, new hires review and agree to all existing policy documents. When policies are updated, re-acceptance is required.

Quarterly, employees participate in KnowBe4 training to ensure they have the most up-to-date security awareness training. Employees also periodically receive simulated phishing campaigns to test their security literacy.

Vulnerability Disclosure

Gradient MSP maintains a Vulnerability Disclosure Program and welcomes submission of vulnerabilities so that they can be fixed.

The program protects the submitter from legal action if the report is made in accordance with the program terms.

For more information, or to report a vulnerability, see our Vulnerability Disclosure Program page.

Configuration Standards

Gradient MSP configures its devices and services using documented configuration standards, based primarily on CIS Benchmarks with additional configuration guidance from vendor recommendations.

These configurations are automatically applied as technology permits and manually reviewed regularly.

Account Provisioning

Within its application, data is associated with an individual account.

Gradient MSP maintains a centralized identity management system for its user accounts. Requests to create new accounts must come from the Human Resources department or via an authorized change request for service or test accounts.

Initial application access is granted based on job descriptions. If additional access is needed, this is requested through Gradient MSP's compliance management system.

Access Control

In its web applications, access requires either a verified email address or identity verification from a third-party provider. Gradient MSP does not store usernames, passwords, or other authentication data for web users.

Internally, access to applications is granted through Gradient MSP's centralized identity platform via SSO. All logon events require multifactor authentication and are monitored for anomalous sign-in requests, such as impossible travel and new geographic locations.

The access must be from a device that meets Gradient MSP's device compliance requirements and initial device login requires multifactor authentication.

Access to critical systems requires connecting from a pre-authorized IP address.

Vulnerability Management

In its web application, Gradient MSP monitors its third-party libraries for known vulnerabilities and updates as needed.

Hosted cloud infrastructure configuration is regularly evaluated for misconfigurations.

Workstations are continuously scanned for patches, both in applications and configuration and updated or reconfigured as new vulnerabilities are identified.

Logging and Monitoring

Gradient MSP maintains logs of both application access and control plane actions, which are monitored for anomalous activity, including known-malicious traffic patterns. This is used both to identify potential security incidents and as a check on management actions.

Internal assets are also monitored for this type of activity and uncommon or anomalous events are reported on.

Email and Web Browser Protections

Email messages are filtered for phishing attempts, malicious links, and malicious files before delivery. Protection against “display name” spoofing is implemented in addition.

Incident Response

Gradient MSP has developed a comprehensive Incident Response plan based on NIST 800-61. This plan outlines specific individuals to contact and actions to take in the event of a potential security incident, including steps to determine escalations.

Additionally, Gradient has arranged for a third-party forensic investigation firm to be available if such services are required.

Penetration Testing

Annually, Gradient MSP undergoes a penetration test against its applications to confirm the efficacy of existing controls and identify areas where security may be strengthened.

Testing is performed by a third-party with limited prior knowledge of the internal infrastructure design.

Regulatory Compliance

Gradient MSP is annually audited against the SOC 2 criteria to independently verify our security policies and controls. The latest version of our public SOC 3 report is available on the Security and Compliance page on our website. The SOC 2 audit results are available on a case-by-case basis with a signed NDA.

Conclusion

Gradient MSP prioritizes security, both internally and in our applications. We are continually looking to improve our security posture, welcome reports of security weaknesses, and encourage anyone with questions to reach out and start a conversation by contacting us at security@meetgradient.com.

Additional Resources:

- Security & Compliance Overview
- SOC 3 Report


gradient
msp