

VERDANT ROBOTICS

IT Manager

HQ - Full Time
Reports to CTO

IT & Internal Systems Engineer – Verdant Robotics

About the role

Verdant Robotics builds AI-powered farming implements. Our Sharpshooter uses computer vision, machine learning and our proprietary Bullseye Technology to weed, thin and fertilize with millimeter accuracy, so farmers grow more with fewer inputs.

Behind the robots is a company that runs on its own infrastructure: the identities and access that let 50+ people do their jobs, the Macs and iPads they work on, the servers and storage in our building, the office and lab networks, the SaaS tools we depend on, and the CI that has to be green for anything to ship. As our IT & Internal Systems Engineer, you will own all of it.

This is a broad role with real ownership and very little bureaucracy. Much of what you're inheriting already works. The job is to keep it healthy, automate what's still manual, and tighten it as we grow. You'll be the person who knows where every account, key and machine is, who closes gaps rather than filing them, and who documents things well enough that nothing depends on one person again.

Your partner role. You'll work alongside our Fleet Infrastructure Engineer, who owns the robot fleet, SaltStack fleet automation, the deployment path and the manufacturing/asset-tracking platform. The two of you sit together and cover for each other. You'll learn enough of the fleet side to keep it running when they're out, and teach your side well enough that they can do the same for you. Neither role is allowed to become a single point of failure.

What you'll do

Identity, access and security

- Own identity and access across AWS IAM, Google Workspace, GitHub, Tailscale, Notion, Slack, Foxglove, OpenAI, Anthropic, Fishbowl and internal services, including onboarding and complete offboarding.
- Sweep our security posture regularly: account and key inventory, secrets handling, patching and access reviews.

Endpoints

- Own the Mac laptop and managed iPad fleet: MDM enrollment, configuration profiles, app deployment, patching, encryption, and the standard build someone gets on day one.
- Keep the iPads healthy in the field too. They're also the operator interface on the robots.

Cloud

- Own AWS for the company: IAM users, roles, policies, MFA and access reviews; CloudTrail and CloudWatch alarms; S3 bucket policy, encryption and lifecycle rules; SSM parameters and secrets; EC2 for internal servers; and cost hygiene via Cost Explorer and Budgets.

- Close standing gaps in our cloud security posture. Configuration recording and access analysis aren't fully deployed yet.

On-prem, CI and networks

- Run our servers, storage, backups, building access and office systems as production services with runbooks.
- Keep GitHub Actions and our self-hosted runners healthy across x64, arm64 and NVIDIA Jetson targets, and unblock builds that break on the runner rather than in the code.
- Manage office and lab networking, Wi-Fi, managed switching, and the Tailscale tag and ACL model that separates internal services from the fleet.
- Own monitoring and alerting for internal services and CI, so problems surface before someone reports them.

People and planning

- Support the team day to day (the laptop, the login, the access request, the printer, the conference room) without letting the interrupt queue swallow project work.
- Write the runbooks that let the next person solve the same problem without you.
- Work with the CTO to plan the security and network architecture we'll need as we grow.

What you bring

- 4+ years in IT, systems or infrastructure engineering, including time as the primary owner of the systems you supported.
- **AWS account ownership.** You've been accountable for an AWS account, not just a user of one. You've written and debugged IAM policies, worked out why a request was denied, cleaned up someone else's users, keys and buckets, set S3 bucket policies and lifecycle rules, used CloudTrail to answer "who did this, and when," and watched the bill. Our footprint is small and unglamorous (IAM, EC2, S3, Lambda, ECR, CloudTrail, CloudWatch, SSM), but you'll own it from day one.
- **Apple fleet management under MDM**, for both macOS and iPadOS: enrollment, configuration profiles, app deployment, patching and disk encryption.
- **Strong Linux administration** of on-prem servers, internal services and CI machines, not only cloud instances.
- **Google Workspace administration:** users, groups, org units, 2SV enforcement and scripted lifecycle management.
- **Scripting habits.** You reach for a script instead of clicking through, write it so others can maintain it, and put it in version control. Any language is fine.
- **CI/CD maintenance**, ideally including self-hosted runners.
- **Practical networking:** LAN, Wi-Fi, managed switching, VPN or mesh networks such as Tailscale, and remote access.
- **Security fundamentals:** access control, secrets handling, patching and least privilege, plus the habit of fixing what you find.
- Clear technical writing, and the judgment to know what needs writing down.
- Calm, methodical work under time pressure, and comfort working hands-on with hardware in our Hayward office.

If you meet most of these but not every one, we'd still like to hear from you. The AWS and Apple MDM experience are the hardest to learn on the job.

Nice to have

- A specific MDM platform (Jamf, Kandji, Mosyle, Intune or similar), Apple Business Manager, and supervised or shared-iPad deployments.

- Configuration management (SaltStack, Ansible, Puppet or Chef) or infrastructure as code (Terraform or similar).
- Running an access-review, key-rotation or audit program with findings tracked to closure.
- Opinions on corporate network and security architecture: segmentation, SSO, managed wireless. We aren't there yet, and you'd help shape it.
- Building internal integrations across tools like Slack, Notion and GitHub.
- IT experience at a hardware, robotics or field-service company, where IT serves production and field operations as well as engineering.

Salary:

\$150,000 ~ \$190,000, plus equity and benefits

How to apply

Email your resume to careers@verdantrobotics.com. A short note about an environment you inherited and what you changed goes a long way.

Verdant Robotics is an equal opportunity employer. We do not discriminate on the basis of race, color, religion, sex, national origin, ancestry, age, disability, medical condition, genetic information, marital status, sexual orientation, gender identity or expression, military or veteran status, or any other status protected by law.