Doppler

Doppler FAQ

Summary

Developers, AI agents, MCP servers, and automated workflows all need secrets to reach the systems your business runs on. If you can't tell which person or agent accessed a secret, you usually find out during an incident or an audit.

Doppler is the secrets manager built for the agentic age. Your people and your AI agents get the secrets they need from one secure place, whether you run on-prem or in the cloud.

Risk reduction and vendor confidence

Q: Does Doppler reduce organizational risk or introduce new exposure?

Doppler replaces scattered, untracked secrets with one platform for your people and your AI agents. It controls who can access each secret and records every change. That lowers the chance of a leak from unmanaged access or human error, including credentials hardcoded into agent scripts.

RESULTS

Less exposure to credential-related incidents, whether access comes from a person or an AI agent

Stronger posture during vendor risk assessments

System-generated records that **support** internal security reviews

CASE STUDY Whatnot has 3,000+ secrets centralized in Doppler across 14 systems, including AWS.

Audit readiness and evidence availability

Q: Today, monitoring access and collecting audit evidence for our secrets posture requires significant manual effort. How does this solution reduce that burden during audits and compliance reviews?

Doppler automatically maintains access logs and change history for sensitive credentials. These records are centralized in a single source, eliminating manual data collection or reliance on individual knowledge. These controls support internal reviews and external audits.

RESULTS

Faster response to audit and compliance requests

Reduced internal effort during security reviews

Consistent evidence year over year

CASE STUDY Triave reduced secret audit times by over 90%.

Enforced ownership and access governance

Q: What controls and visibility are in place today for managing access and credential changes, and how is associated risk assessed?

Doppler enforces granular access controls with defined permissions and reviewable change history. Access can be granted, reviewed, or revoked in a controlled manner without relying on ad hoc processes.

RESULTS

- **Clear enforcement** of least-privilege access
- **More reliable** offboarding and role changes
- **Visibility and approved workflows** for sensitive and mission critical secrets
- **Reduced long-term risk** from unmanaged access

CASE STUDY MATTR adopted Change Requests totaling ~300 approvals in one month.

Long-term fit and scalability

Q: Are our sensitive credentials being managed with enterprise-level governance and security in mind? How does pricing scale?

Doppler is built to meet enterprise security and compliance expectations from day one with ISO 27001 and SOC II compliance. As organizational requirements expand, additional governance, approval workflows, and oversight can be applied without changing platforms or vendors.

Pricing scales in line with organizational usage, without unexpected cost increases as teams and environments expand.

RESULTS

- **No compromise** on enterprise security requirements
- **Reduced the likelihood** of future vendor replacement
- Supports consistent access and governance controls **at scale**

CASE STUDY BODI scaled to roll out to 50 systems for company-wide adoption.

AI agents

Q: How does Doppler manage secrets for AI agents?

Doppler's MCP server lets AI agents pull the secrets they need directly, so you don't have to write custom scripts or hardcode credentials. You can also sync secrets into the GitHub Copilot agent and set OpenAI keys to rotate automatically.

CASE STUDY Ada used Doppler to boost efficiency for secrets management by 95%.

One platform for every secret your developers and AI agents need

Your developers and AI agents get their secrets from one secure place, on-prem or in the cloud.

Get a Demo → **Learn More**