SENDSAFELY

How Unity Keeps Secrets a Secret with SendSafely

Unity®

Unity, the world-renowned platform for real-time 3D content development, uses SendSafely to secure sensitive data across internal teams and external communications. From bug reporting to engineering collaboration, Unity relies on SendSafely as its universal, tool-agnostic solution for managing secrets, keeping them out of tools such as email, Slack, Zendesk, and Jira.

The Challenge

Unity's DevOps and Customer Support teams routinely exchange sensitive credentials, API keys, and proprietary files, both internally and with external contributors or customers. Their existing tools, including email, Slack, Zendesk and Jira, aren't designed for the level of secure data handling Unity required. Additionally, audit compliance with SOX, SOC 2 and GDPR regulations required strict control over how data is stored, shared, and retained, regardless of the platform used.

Unity needed a solution that:

- Prevents secrets from living in third-party systems
- Supports external collaboration without compromising security
- Maintains compliance for internal and external audits.

The Solution

Unity adopted SendSafely to securely transmit and store sensitive data inside and outside the organization. Two key use cases emerged:

1. Secure External Collaboration

Unity's Customer Engagement Team uses SendSafely Workspaces to collect and store sensitive customer data during the support process:

- A Workspace is associated with a specific customer ticket, and folder names within the Workspace are automatically generated based on the corresponding bug or issue
- Bug-related files and other artifacts are gathered from customers by sharing the link to the SendSafely Workspace
- Support engineers are automatically provisioned access to the Workspace files via automation

For more information on how your business can benefit from SendSafely or to start a free trial, go to www.sendsafely.com or email sales@sendsafely.com.

"SendSafely is the universal tool for storing and sharing sensitive data across the organization - no matter what tool you're in."

- Alix Roberts, DevOps Manager at Unity

Benefits:

- Secure, shared access to support artifacts for multiple teams of engineers, improving collaboration
- Keeps sensitive customer content out of Jira and Zendesk, ensuring compliance and minimizing risk
- Handles large files easily, including code and binary files. *"SendSafely handles it all." — Alix Roberts, DevOps Manager at Unity*

2. Secure Internal Collaboration

Across Unity's technical teams, each group maintains its own secure secrets store containing passwords, API keys, and configuration files. When temporary access credentials need to be shared beyond a team, for example, with another group or a contractor, SendSafely is the standard tool. Key features used include:

- Automatic expiration and deletion
- Access limits to control how many times a package can be opened
- Detailed tracking of views/accesses

SendSafely ensures secrets "stay secret", even when shared across the org.

"We have a need to share secrets in a way that does not expose them to the tooling, such as Slack, email, articles, documentation, etc."

— Alix Roberts, DevOps Manager at Unity

Conclusion

SendSafely helps Unity scale secure communication and collaborator without compromising speed or compliance. From internal DevOps teams to customer support, SendSafely ensures Unity's secrets stay secret - everywhere. "It's one of those tools that just works - everyone is happy. You can't get higher praise than that." — Alix Roberts

Secure data workflows across Unity's
internal and external support processes

Minimal Friction for users;
the tool "just works"

End-to-end Compliance
with SOX, SOC2, and GDPR, regardless of where or how data is accessed.

For more information on how your business can benefit from SendSafely or to start a free trial, go to www.sendsafely.com or email sales@sendsafely.com.