

NOLS Eliminates Shadow IT and Gains Control Over File Sharing with Wing Security

Description

 **Employees:** 750

 **Location:** Wyoming, USA

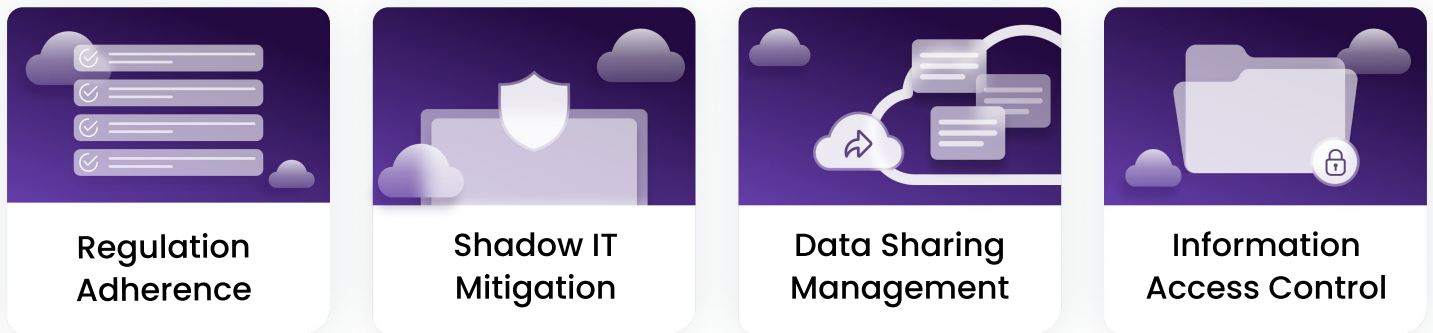
 **Industry:** Non-profit

National Outdoor Leadership School (NOLS) is a renowned non-profit organization established in 1965, dedicated to teaching leadership and wilderness skills through outdoor expeditions and courses. With over five decades of experience, NOLS has developed a reputation for excellence in outdoor education, providing programs worldwide.

Overview

NOLS adopted Wing to address key security challenges, with a strong focus on gaining more visibility into their SaaS stack. Through Wing, NOLS optimized their SaaS application usage to reduce unnecessary costs associated with duplicate or redundant apps. This effort not only enhanced security and operational visibility but also brought financial benefits by refining resources and reducing unnecessary expenditures on overlapping software solutions.

The Challenges



NOLS faced a few significant security challenges in which they had to address security vulnerabilities while gaining comprehensive visibility and control over SaaS usage. The lack of oversight made it difficult to monitor SaaS security threats and comply with regulations, exacerbated by the proliferation of shadow IT and unnecessary apps. Additionally, they struggled with managing internal and external data sharing while enforcing strict permission controls to protect sensitive information. To address these issues, NOLS adopted Wing Security to enhance IT governance, streamline operations, and bolster data security.

Lack of Visibility and Control

According to Michael Hess, Cloud Infrastructure Manager at NOLS, the team grappled with questions such as “What applications are our users actually using that they haven’t disclosed? Where is data being stored that we don’t know about?” This lack of centralized control led to the extensive use of unsanctioned applications, which concealed where sensitive data was stored or accessed, increasing security vulnerabilities and compliance risks. Consequently, IT administrators struggled to effectively track and manage the organization’s SaaS stack.

Uncontrolled Data Sharing

NOLS faced challenges with data-sharing practices across their Google Workspace. Additionally, the large number of contractors led to numerous stale accounts cluttering their GitHub repositories, further complicating management and raising security concerns. Wing’s capabilities allowed NOLS to identify and manage stale accounts effectively, ensuring that access permissions were promptly revoked when no longer needed. Moreover, it provided controls to restrict unnecessary public sharing of Git repositories, thereby enhancing data protection measures and aligning with compliance requirements.

The Solution

Connecting NOLS to Wing was smooth, taking only a day for setup. NOLS wasted no time in leveraging **Wing's automation for file-sharing alerts and application monitoring**, significantly enhancing its security posture. **By promptly notifying users about forbidden apps and automating token revocations**, the team was prepared to manage potential security breaches and increase compliance awareness. This proactive approach required minimal time investment, approximately 10 to 15 minutes every few days, allowing NOLS to focus resources where they were most needed during security incidents.



"If I spend an hour a week in Wing, that's a lot. I would say it's maybe 10, 15 minutes every couple of days."

Michael Hess

Cloud Infrastructure Manager

How NOLS Benefits From Wing



Significant Cost Savings and Optimization

Wing provided NOLS with comprehensive visibility into their SaaS application landscape, uncovering over 50 duplicate or redundant applications. This discovery enabled NOLS to consolidate their application portfolio, ensuring the adoption only of solutions that met security and compliance standards. The consolidation resulted in estimated annual cost savings of tens of thousands of dollars while ensuring proper licensing, access controls, and compliance adherence.

By streamlining their application portfolio, NOLS not only reduced expenses but also simplified the management of their SaaS environment.

Discovering and Categorizing SaaS Applications

Wing Security enabled NOLS to conduct a thorough scan and categorization of all SaaS applications used within the organization. This effort created a comprehensive inventory of sanctioned and unsanctioned applications, prioritizing those needing immediate attention.

Managing Data Sharing and Oversharing Risks

Using Wing Security's automation, NOLS implemented rules to alert users about prohibited applications, revoke access tokens, and restrict file-sharing permissions. These measures significantly reduced sensitive data exposure risks, ensuring better compliance with internal and external security policies.

Proactive Threat Intelligence and Response

Wing's SSPM solution gave NOLS timely breach and security alerts for applications in their SaaS stack, enabling swift responses to mitigate risks effectively. This proactive approach safeguarded the integrity and confidentiality of their data, ensuring continuous protection against emerging threats.

Key Takeaways

By implementing Wing Security, NOLS successfully tackled the challenges of shadow IT and uncontrolled data sharing. Wing's SSPM solution provided the necessary tools to discover and manage SaaS applications, enforce security policies, and enhance overall data protection. With improved visibility, control, and automation, NOLS ensured the use of only applications with sufficient security standards, optimized their SaaS application usage, and ensured a secure environment for their operations.



"Wing allowed us to discover exactly what was being used out there, why, and by whom."

Tim Yaley

Cloud Engineer

