NROC Security
Customer Case Study

Securing GenAI to unleash personal productivity and innovation

Introduction

A city tours and cruise company is best known for operating various tourist experiences on many iconic sites. Their 5,000+ staff serve more than 20 million customers across 50 U.S. cities and 10 countries. Besides the consumer business, this company is also a diversified technology and professional services organization operating equipment manufacturing, maintenance and consulting businesses.

The organization had a comprehensive AI agenda that covered in-house developed AI/ML for business specific use cases, AI for customer service, as well as encouraged employees to use public LLMs for personal productivity.
The technology and security leadership recognized very early on the security issues related to the usage of the emerging GenAI technologies. Early red-teaming showed evidence of data leakages, which initiated exploration and prototyping of security solutions to address the emerging issues.

NROC Security has been collaborating with the city tours and cruise company on innovative solutions for securing employee use of GenAI apps.

Challenges

The city tours and cruise company encountered a triple challenge when empowering employees to use GenAI for personal productivity:

Lack of insights into the actual use cases
No existing security solution provided information about active users, apps and prompts submitted, which made it impossible to assess risks, guide end users and drive the productivity agenda.

Data leakage risks
Employees used tools like ChatGPT for daily tasks. However, without proper oversight, these tools posed a risk of exposing classified data or personally identifiable information (PII).

Ease of managing solutions across the heterogeneous enterprise
The company has grown through acquisitions and therefore, had better control over identities and networks. The workstation images were less standardized, which would have made any end point based security solution very difficult to deploy.

"I can be more lenient with what employees can do with GenAI, because I have full visibility into usage and all personally identifiable information gets Xed out from the prompts."

DIRECTOR AND DEPUTY CISO, CITY TOURS AND CRUISE COMPANY

Solution

To address these challenges, the company implemented NROC Security, a comprehensive governance and guardrail solution designed specifically to bridge the gap between employee productivity and enterprise-grade data protection in the context of GenAI usage.

Insights into how employees use GenAI
NROC Security provided the city tours and cruise company with insights into how GenAI tools like ChatGPT were being used across the organization:

- Every usage of GenAI apps was authenticated on a company ID, even when the end user is using private/free app on a personal ID
- The best use cases and most proficient prompters were identified and can be promoted across the organization
- Reporting provided real-time data for risk assessment, governance of the app portfolio and for optimizing license purchases of commercial GenAI apps

Protection against data leakage with real-time end user guidance
A unique feature of NROC Security's platform was its ability to protect against data exposure in the GenAI app's native user experience and to guide users when classified content was detected:

- Over 10,000 prompts per month were monitored and analyzed, most on ChatGPT
- Over 4,000 pieces of content were redacted every month, mostly classified content like PII or company identifiers
- Users were supported with real-time guardrails: 7.5% of interactions triggered 'block' or 'are you sure?' actions, reminding the users to exercise caution with GenAI apps

Ability to identify and take action on risky users
With NROC Security's robust analytics, the city tours and cruise company gained the ability to proactively detect and manage high-risk behaviors:

- Risk-based analytics identified that just 3% of users were responsible for over half of all detections of PII
- Insights allowed the security team to implement targeted education and remediation strategies, significantly reducing organizational risk with minimal disruption
- User group based policies in the solution can be used to allow/disallow GenAI usage for non-compliant employees

Deployment with no end point plugin or agent installations
For a heterogeneous enterprise environments, a network based solution was faster to deploy than any end point based alternative:

- Proxy auto-configuration setting and certificate was deployed using a Group Policy Object. User authentication was realized with a standard SSO with no end point dependency
- No interoperability testing was needed against any pre-existing end point software, agents or browser plugins

Conclusion

GenAI for employee productivity is a learning-by-doing endeavour for both the employees and security leaders. Successful adoption required freedom for employees to explore how GenAI can help them get more done, faster. At the same time, the security team needed to mitigate the known security risks. NROC Security helped this organization strike the right balance.

By combining deep visibility, real-time data protection, and intelligent user guidance, NROC Security transformed personal productivity GenAI from a security risk and governance challenge into a channel for responsible innovation.

To learn how NROC Security can safely accelerate GenAI usage, productivity and innovation of your employees, visit www.nrocsecurity.com.