CYBERHAVEN

Dynamic DLP Reduces Accidental Insider Threats

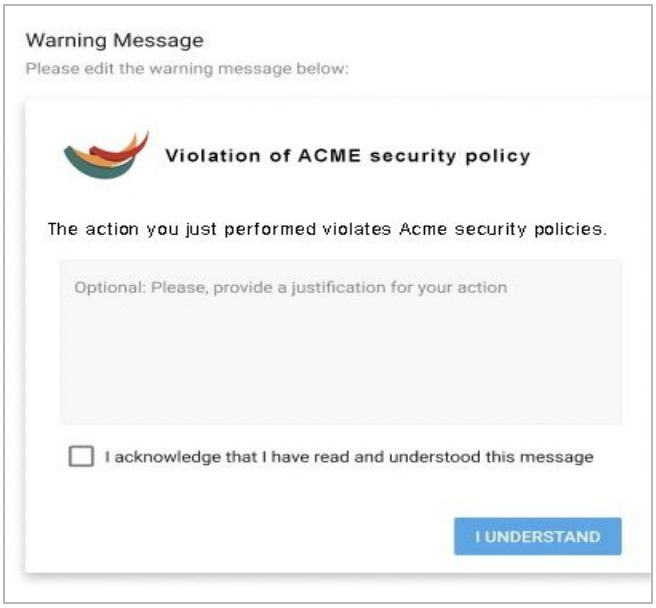
Just-in-Time security training prevents Insider Threats

People make mistakes. According to Egress' 2020 Insider Threat Report, "78% say employees have put data at risk accidentally". Many times users are not aware that they are violating corporate security policies. All organizations need better ways to educate and train their users on security policy secure ways to transmit sensitive data.

With Cyberhaven you can configure Just-in-Time intervention actions to train users. This is the most effective way to educate users - when they are in the act of breaking corporate policies. The actions you can take with Cyberhaven range from displaying warnings to end-users to blocking, closing apps, and locking out repeat offenders from their session if necessary. Users will respond with a new awareness of clear alternatives and consequences. The goal is to educate users with security best practices.

Benefits of Cyberhaven:

- Educate users as to why certain data is sensitive
- Create user awareness of why a certain application or website is risky
- Flexibility to configure rules for each dataset individually or for all sensitive datasets
- Configure custom categories of exfiltration locations such as website domains, email domains or cloud services, endpoint apps, etc.
- Dynamic data tracing follows all your data



Dynamic Data Protection

Just-in-Time training with real-time responses helps users to increase their security awareness and correct mistakes immediately. Cyberhaven's continuous data tracing delivers dynamic data protection for all data and all users all the time.