The NJD is seeking an on prem COTS solution that can enable the Court to meet the criteria outlined in the Judiciary IT Security Score Card for its 300 end-users. The Court is required to reduce risk; detect and respond to threats; and prove regulatory compliance. Varonis focuses on all aspects of an organizations data to mitigate risk and secure data from the inside out. Real-time monitoring access, tagging data, auditing file touches, and alerting on abnormal system behavior allowing the Court to gain full visibility on where our data is being accessed at any given time. The software must:

- Identifying overexposed sensitive data on the network (i.e. PII, Confidential, Court documentation)
- Visualizing who has access on multiple servers / platforms
- Auditing / sorting through all file touches (who is doing what, when and where)
- Data Categorization;
- Reporting on user access / sensitive data and automating report creation
- Automating governance process – who should and should not have access
- Alerting on abnormal behavior (i.e. sensitive data copied) / integration w/ SIEM
- Automating response to cyber-attacks like malware/ransomware
- Incident response support to investigate/remediate threats